

RESEARCH OUTPUTS / RÉSULTATS DE RECHERCHE

La protection des données à caractère personnel en droit européen

Herveg, Jean; Van Gyseghem, Jean-Marc

Published in:

Journal européen des droits de l'homme / European Journal of Human Rights

Publication date:

2018

Document Version

le PDF de l'éditeur

[Link to publication](#)

Citation for pulished version (HARVARD):

Herveg, J & Van Gyseghem, J-M 2018, 'La protection des données à caractère personnel en droit européen: chronique de jurisprudence 2017', *Journal européen des droits de l'homme / European Journal of Human Rights*, Numéro 1, p. 3-51.

General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal ?

Take down policy

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

La protection des données à caractère personnel en droit européen – Chronique de jurisprudence (2017)

Personal data protection in European Law – Column of case-law (2017)

Jean Herveg & Jean-Marc Van Gyseghem¹

Résumé

La chronique analyse la contribution des juridictions de l'Union européenne et de la Cour européenne des droits de l'homme à la protection des données à caractère personnel pour l'année 2017.

La jurisprudence de la Cour européenne des droits de l'homme a concerné la surveillance des individus et de leurs communications, la saisie de données électroniques, la protection contre la divulgation de données, la protection des données relatives à la santé, des données biométriques, bancaires et fiscales, la filiation, l'équilibre entre liberté d'expression, vie privée et réputation, ainsi que le droit d'accès des individus aux données détenues par des autorités publiques. La jurisprudence des juridictions de l'Union européenne, moins étoffée que celle de Strasbourg, a porté sur plusieurs aspects de la directive 95/46 tels que son champ d'application matériel, le droit de recours juridictionnel et la conservation des données.

Abstract

This column analyses the contribution from the European Court of Human Rights and European Union jurisdictions to data protection in 2017.

The cases brought before the European Court of Human Rights concern the monitoring of individuals and their communications, the disclosure of personal data, the seizure of electronic data, the protection of medical data, biometric data, bank data and tax data, filiation matters, the balance between freedom of speech, privacy, and reputation, and the right of access to personal data. Case law from the European jurisdictions provided the opportunity to deal with various aspects of Directive 95/46, including its scope rationae materiae, effective judicial remedy, and personal data retention.

I. La protection des données dans la jurisprudence de la Cour européenne des droits de l'homme

A. LA RECONNAISSANCE EXPLICITE D'UN DROIT À L'AUTODÉTERMINATION INFORMATIONNELLE

Pour la première fois, la Cour européenne des droits de l'homme a fait mention de l'existence d'un droit à l'autodétermination informationnelle en énonçant ce qui suit²:

«L'article 8 de la Convention consacre donc le droit à une forme d'autodétermination informationnelle, qui autorise les personnes à invoquer leur droit à la vie privée en ce qui concerne des données qui, bien que neutres, sont collectées, traitées et diffusées à la collectivité, selon des formes ou modalités telles que leurs droits au titre de l'article 8 peuvent être mis en jeu».

B. LA PROTECTION CONTRE LES MESURES DE SURVEILLANCE

1. *Le principe de la confidentialité de toutes les communications*

L'article 8 protège la confidentialité de toutes les communications entre les individus³.

Le droit au respect de la correspondance protège la confidentialité des communications privées, quel que puisse être le contenu de la correspondance concernée et quelle que puisse être la forme qu'elle prend. Ceci signifie que l'article 8 protège la confidentialité de tous les échanges qui peuvent intervenir entre des individus à des fins de communication⁴.

Conformément à la jurisprudence de la Cour, les appels téléphoniques depuis des locaux commerciaux, en ce compris le bureau d'une fonctionnaire d'État, sont couverts par les notions de vie privée et de correspondance. Les e-mails et toutes communications échangées via un compte de messagerie instantanée depuis le lieu du travail sont de même protégés, de la même façon que les informations tirées du contrôle de l'utilisation privée de l'Internet⁵.

¹ This work has been done with the financial support from the European Union's Horizon 2020 research and innovation program under Grant Agreements n° 688520 (TeSLA) & 730953 (Inspex) and in part by the Swiss Secretariat for Education, Research and Innovation (SERI) under Grant 16.0136 730953. La publication ne reflète que l'opinion de ses auteurs et la Commission européenne ne peut être tenue responsable de l'usage qui en serait fait.

² Cour eur. D.H. (GC), arrêt du 27 juin 2017, n° 931/13, *Satakunnan Markkinapörssi Oy et Satamedia Oy c. Finlande*, § 137.

³ Cour eur. D.H., arrêt du 15 juin 2017, n° 21979/08, *Oderovs c. Lettonie*, § 51; arrêt du 7 novembre 2017, n° 37717/05, *Dudchenko c. Russie*, § 104.

⁴ Cour eur. D.H., arrêt du 31 octobre 2017, n° 22767/08, *Dracos Ioan Rusu c. Roumanie*, § 33.

⁵ Cour eur. D.H., arrêt du 19 janvier 2017, n° 63638/14, *Posevini c. Bulgarie*, § 75; arrêt du 7 novembre 2017, n° 21200/05, *Akhlyustin c. Russie*, § 37.

2. L'ingérence et le test des attentes raisonnables de vie privée

La Cour a recours au test des *attentes raisonnables de vie privée* pour décider s'il y a ingérence dans le droit au respect de la vie privée. Le test n'est toutefois pas décisif même s'il s'agit d'un élément important d'appréciation de l'existence d'une ingérence⁶.

En règle, l'enregistrement systématique ou permanent de données suscite des questions de vie privée même si cet enregistrement vidéo ou audio est réalisé lorsque la personne se trouve dans un endroit public⁷.

Le requérant peut se prévaloir d'une attente raisonnable de vie privée dans son bureau (en ce compris pour tout appel téléphonique réalisé depuis son bureau) lorsqu'il n'a pas été prévenu par son employeur que son bureau pourrait être filmé ou que ses appels téléphoniques pourraient être interceptés. Dans le cas d'espèce, la Cour a retenu que le requérant avait aussi été filmé, que les enregistrements avaient été conservés et examinés par des tiers, sans que le requérant ne le sache et sans qu'il n'y ait consenti, et que les enregistrements ont été utilisés à titre de preuve dans des procédures pénales⁸.

L'interception de la correspondance représente une ingérence qui doit être justifiée⁹.

L'interception des communications téléphoniques constitue une ingérence dans l'exercice des droits protégés par l'article 8. Les conversations téléphoniques sont couvertes par les notions de vie privée et de correspondance¹⁰.

L'interception *indirecte* de communications téléphoniques constitue aussi une ingérence au regard de l'article 8. Ceci signifie que l'interlocuteur d'une personne placée sur écoute téléphonique doit jouir de la même protection que cette dernière¹¹.

La mise sous écoute téléphonique du requérant et sa surveillance constituent tout autant une ingérence dans le droit de la vie privée de la correspondance¹².

La surveillance vidéo secrète du requérant alors qu'il se trouvait dans des lieux privés où ses attentes de vie privée étaient élevées, l'enregistrement de données

⁶ Cour eur. D.H., arrêt du 7 novembre 2017, n° 21200/05, *Akhlyustin c. Russie*, § 38.

⁷ *Ibid.*, § 38.

⁸ *Ibid.*, § 39.

⁹ Cour eur. D.H., arrêt du 31 octobre 2017, n° 22767/08, *Dracos Ioan Rusu c. Roumanie*, § 34.

¹⁰ Cour eur. D.H., arrêt du 7 novembre 2017, n° 29431/05, *Zubkov et autres c. Russie*, § 120; arrêt du 7 novembre 2017, n° 44045/05, *Y. Moskaiev c. Russie*, § 35.

¹¹ Cour eur. D.H., arrêt du 17 janvier 2017, n° 6656/10, *Ayfer Erdogan c. Turquie*, § 42.

¹² Cour eur. D.H., arrêt du 7 février 2017, n° 35285/08, *Irfan Güzel c. Turquie*, § 80; arrêt du 4 avril 2017, n° 2742/12, *Matanovic c. Croatie*, § 112; arrêt du 7 novembre 2017, n° 59589/10, *K. Moskaiev c. Russie*, § 45; arrêt du 23 novembre 2017, n° 47074/12, *Grba c. Croatie*, § 84. Sur la mise sous écoute d'un magistrat apparemment indelicat, voy.: l'arrêt du 29 juin 2017, n° 33242/12, *Terrazoni c. France*.

à caractère personnel, l'analyse de ces enregistrements par des tiers sans que le requérant ne l'ait su ou qu'il n'y ait consenti, et l'utilisation de ces enregistrements vidéos à titre de preuve dans des procédures pénales, constituent une ingérence dans le droit au respect de sa vie privée¹³.

Les fouilles réalisées par la police dans des e-mails ne constituent pas une ingérence dans le droit au respect de la vie privée du requérant dès lors que la police n'a pu le faire qu'en raison du fait que la personne avait donné son mot de passe aux policiers et les avait invités à le faire et ce, sans qu'il n'y ait de traces qu'il y aurait été contraint de le faire comme c'eût été le cas si les policiers lui avaient fait comprendre qu'il n'avait pas d'autre choix que d'autoriser la police à accéder à son compte ou qu'elle le ferait de toute façon. Le fait qu'il ait été emmené menotté au commissariat de police et qu'il y ait été emprisonné, ne modifie pas par lui-même cette conclusion¹⁴.

Pour rappel, pour être admissible, l'ingérence doit être prévue par la loi, poursuivre un but légitime et être nécessaire dans une société démocratique¹⁵.

3. La qualité de la loi en matière de surveillance secrète

Être prévue par la loi signifie que la mesure contestée doit avoir une base en droit national et être compatible avec le principe de la primauté du droit. La loi doit donc répondre à des exigences de qualité: elle doit être accessible à la personne concernée et être prévisible dans ses effets¹⁶.

La Cour a rappelé que l'exigence de prévisibilité dans le contexte des interceptions téléphoniques ne se concevait pas de la même façon que dans les autres domaines. En matière de surveillance secrète, elle ne signifie pas que la personne doit être capable de prévoir quand les autorités sont susceptibles d'intercepter ses communications afin de pouvoir adapter son comportement en conséquence. Toutefois, le risque d'arbitraire est évident surtout quand un pouvoir conféré au pouvoir exécutif s'exerce en secret. Il est alors essentiel d'avoir des règles claires et détaillées sur l'interception des conversations téléphoniques, en particulier quand les technologies disponibles deviennent de plus en plus sophistiquées. Le droit national doit être suffisamment clair pour donner aux citoyens une indication appropriée quant aux circonstances et conditions dans lesquelles les autorités publiques sont autorisées à recourir à de telles mesures¹⁷.

¹³ Cour eur. D.H., arrêt du 7 novembre 2017, n° 29431/05, *Zubkov et autres c. Russie*, § 121.

¹⁴ Cour eur. D.H., arrêt du 19 janvier 2017, n° 63638/14, *Posevini c. Bulgarie*, § 75.

¹⁵ Cour eur. D.H., arrêt du 7 novembre 2017, n° 29431/05, *Zubkov et autres c. Russie*, § 122; arrêt du 7 novembre 2017, n° 44045/05, *Y. Moskaiev c. Russie*, § 36; arrêt du 7 novembre 2017, n° 59589/10, *K. Moskaiev c. Russie*, § 46.

¹⁶ Cour eur. D.H., arrêt du 29 juin 2017, n° 33242/12, *Terrazoni c. France*, § 45; arrêt du 31 octobre 2017, n° 22767/08, *Dracos Ioan Rusu c. Roumanie*, § 35; arrêt du 7 novembre 2017, n° 29431/05, *Zubkov et autres c. Russie*, § 123; arrêt du 7 novembre 2017, n° 44045/05, *Y. Moskaiev c. Russie*, § 38; arrêt du 7 novembre 2017, n° 59589/10, *K. Moskaiev c. Russie*, § 47.

¹⁷ Cour eur. D.H., arrêt du 31 octobre 2017, n° 22767/08, *Dracos Ioan Rusu c. Roumanie*, § 35.

De plus, dès lors que la mise en œuvre de mesures secrètes de surveillance des communications n'est pas susceptible d'être contrôlée par les personnes concernées ni par le public en général, il serait contraire au principe de la primauté du droit que le pouvoir discrétionnaire conféré au pouvoir exécutif ou à un juge soit libellé dans des termes d'un pouvoir illimité. En conséquence, la loi doit indiquer l'étendue de ce pouvoir discrétionnaire et la manière de l'exercer, avec suffisamment de clarté pour donner aux individus une protection adéquate contre les ingérences arbitraires¹⁸.

La Cour a rappelé les protections minimales suivantes qui doivent être reprises dans la loi afin d'éviter tout abus de pouvoir :

- la nature des infractions qui peuvent donner lieu à un mandat d'interception ;
- la détermination des catégories de personnes susceptibles d'avoir leur téléphone mis sous écoute ;
- la durée limitée de l'écoute téléphonique ;
- la procédure à suivre pour analyser, utiliser et conserver les données ainsi obtenues ;
- et les circonstances dans lesquelles les enregistrements peuvent ou doivent être effacés ou détruits.

4. *Le caractère nécessaire de la mesure de surveillance secrète dans une société démocratique*

La Cour reconnaît aux autorités nationales une marge d'appréciation dans le choix des moyens mis en œuvre pour protéger la sécurité nationale. Toutefois, cette marge d'appréciation est soumise à un contrôle européen qui couvre tant la législation que les décisions qui la mettent en œuvre. Au vu du risque posé par un système de surveillance secrète destiné à protéger la sécurité nationale d'affaiblir voire de détruire la démocratie au motif de la protéger, la Cour doit être convaincue qu'il existe des protections adéquates et effectives contre les abus¹⁹.

Une ingérence sera considérée comme nécessaire dans une société démocratique à un objectif légitime si elle répond à un besoin social impérieux et, en particulier, si elle est proportionnée à l'objectif légitime poursuivi et si les raisons avancées par les autorités nationales pour la justifier sont pertinentes et suffisantes. S'il incombe aux autorités nationales de réaliser cette première évaluation dans tous ses aspects, le contrôle final du caractère nécessaire de l'ingérence revient à la Cour.

En matière de surveillances secrètes, cette appréciation dépend de toutes les circonstances de la cause comme la nature, l'étendue et la durée des mesures de

¹⁸ *Idem*.

¹⁹ Cour eur. D.H., arrêt du 29 juin 2017, n° 33242/12, *Terrazzoni c. France*, §§ 53-54 ; arrêt du 31 octobre 2017, n° 22767/08, *Dracos Ioan Rusu c. Roumanie*, § 35 ; arrêt du 7 novembre 2017, n° 21200/05, *Akhlyustin c. Russie*, § 41 ; arrêt du 7 février 2017, n° 35285/08, *Irfan Güzel c. Turquie*, § 85.

surveillance, les raisons de les ordonner, les autorités compétentes pour les autoriser, les réaliser et les contrôler, ainsi que le type de recours fourni par le droit national. La Cour doit vérifier si les procédures qui encadrent l'autorisation et la mise en œuvre de ces mesures restrictives permettent de limiter l'ingérence à ce qui nécessaire dans une société démocratique²⁰.

La loi ne présente pas une qualité suffisante lorsque les dispositions légales qui régissent l'interception des communications n'offrent pas des garanties appropriées et effectives contre l'arbitraire et le risque d'abus. Elles sont dès lors incapables de maintenir l'ingérence à ce qui est nécessaire dans une société démocratique. L'appréciation de la qualité de la loi par la Cour implique nécessairement un certain degré d'abstraction. Toutefois, il ne peut pas s'agir du même degré d'abstraction lorsque le requérant se plaint de mesures spécifiques et incontestées de surveillance secrète. Dans cette hypothèse, la Cour doit, en règle, porter son attention, non pas sur la loi en tant que telle, mais sur la manière dont elle a été appliquée au requérant dans le cas d'espèce²¹.

Il faut en premier que le juge vérifie l'existence de soupçon raisonnable à l'encontre de la personne à surveiller²².

Il y a violation de l'article 8 lorsque les juridictions nationales ne vérifient pas l'existence de soupçons raisonnables, ainsi que lorsqu'elles ne vérifient pas le caractère nécessaire de la surveillance dans une société démocratique – ni la proportionnalité de la mesure²³.

La décision autorisant l'ingérence doit contenir des indications qui permettent de savoir si le juge a vérifié si la mesure était nécessaire dans une société démocratique et, en particulier, s'il a vérifié la proportionnalité de l'ingérence par rapport au but légitime poursuivi. Il n'est pas suffisant d'indiquer dans l'ordonnance qu'il semble impossible d'obtenir autrement les informations recherchées sans expliquer comment le juge est arrivé à cette conclusion. Ce type d'affirmation vague et générale est insuffisant pour justifier la décision d'autoriser une longue surveillance secrète dans le temps (180 jours) qui entraîne une ingérence grave dans le droit au respect de la vie privée et de la correspondance²⁴.

L'absence de raisonnement dans le mandat du juge d'instruction relatif aux circonstances particulières du cas d'espèce et, en particulier, les raisons pour lesquelles les investigations ne pouvaient pas être réalisées par des moyens moins intrusifs,

²⁰ Cour eur. D.H., arrêt du 7 novembre 2017, n° 29431/05, *Zubkov et autres c. Russie*, § 124; arrêt du 7 novembre 2017, n° 44045/05, *Y. Moskaev c. Russie*, § 38; arrêt du 7 novembre 2017, n° 59589/10, *K. Moskaev c. Russie*, §§ 48, 50.

²¹ Cour eur. D.H., arrêt du 7 novembre 2017, n° 44045/05, *Y. Moskaev c. Russie*, § 40; arrêt du 7 novembre 2017, n° 37717/05, *Dudchenko c. Russie*, § 95; arrêt du 7 novembre 2017, n° 59589/10, *K. Moskaev c. Russie*, § 50.

²² Cour eur. D.H., arrêt du 7 novembre 2017, n° 37717/05, *Dudchenko c. Russie*, § 97.

²³ Cour eur. D.H., arrêt du 7 novembre 2017, n° 37717/05, *Dudchenko c. Russie*, § 98; arrêt du 7 novembre 2017, n° 44045/05, *Y. Moskaev c. Russie*, § 41.

²⁴ Cour eur. D.H., arrêt du 7 novembre 2017, n° 37717/05, *Dudchenko c. Russie*, § 98.

à laquelle s'ajoute le fait que les juridictions nationales ont justifié *a posteriori* le recours à la surveillance secrète, n'était pas conforme au droit national et n'offrait pas les protections appropriées contre les différents abus possibles. La Cour a souligné en particulier le fait que le droit national tel qu'interprété et appliqué par les juridictions compétentes ne fournissait pas de clarté raisonnable quant à l'étendue et la manière d'exercer le pouvoir discrétionnaire conféré aux autorités publiques et, en particulier, n'offrait pas en pratique de protections adéquates contre les différents abus possibles²⁵.

Le service qui délivre l'autorisation doit être à même de vérifier l'existence d'un soupçon raisonnable à l'égard de la personne concernée, en particulier de rechercher s'il existe des indices permettant de la soupçonner de projeter, de commettre d'avoir commis des actes délictueux ou d'autres actes susceptibles de donner lieu à des mesures de surveillance secrète, comme par exemple des actes mettant en péril la sécurité nationale. Ce même service doit s'assurer que l'interception requise satisfait aux critères de nécessité dans une société démocratique notamment que l'ingérence est proportionnée au but légitime poursuivi, en vérifiant par exemple s'il est possible d'atteindre les buts recherchés par des moyens moins intrusifs²⁶.

Il y a violation de l'article 8 quand le juge qui autorise la prolongation d'une écoute téléphonique ne réalise pas un contrôle judiciaire de la décision de la police de mettre le téléphone du requérant sous écoute. Pour le dire autrement, il y a violation de l'article 8 lorsqu'aucune autorité (indépendante des autorités qui ont réalisé la mise sur écoute) n'a évalué la justification du recours à la procédure urgente pour la mise sous écoute téléphonique, ni si la décision était fondée sur un soupçon raisonnable que le requérant aurait commis un acte criminel ou que cette mise sous écoute était nécessaire dans une société démocratique et, en particulier, si elle était proportionnée au but légitime qui aurait été poursuivi. En conséquence, la mise sous écoute des communications du requérant par le biais de la procédure urgente n'était pas accompagnée des protections adéquates contre l'arbitraire²⁷.

Si la Cour reconnaît que les services secrets peuvent exister de manière légitime dans une société démocratique, elle répète que les pouvoirs de surveiller secrètement les citoyens ne sont admissibles sous la Convention que dans la mesure de ce qui est strictement nécessaire pour protéger des institutions démocratiques²⁸.

²⁵ Cour eur. D.H., arrêt du 4 avril 2017, n° 2742/12, *Matanovic c. Croatie*, §§ 113-114; arrêt du 23 novembre 2017, n° 47074/12, *Grba c. Croatie*, §§ 85-86 (voy. le § 89 et s. pour la question de la provocation à commettre des actes illicites).

²⁶ Cour eur. D.H., arrêt du 7 février 2017, n° 35285/08, *Irfan Güzel c. Turquie*, § 86.

²⁷ Cour eur. D.H., arrêt du 7 novembre 2017, n° 59589/10, *K. Moskalev c. Russie*, §§ 52-53.

²⁸ Cour eur. D.H., arrêt du 18 juillet 2017, n° 27473/06, *Mustafa Sezgin Tanrikulu c. Turquie*, § 42.

5. *L'accès à la décision autorisant la surveillance secrète*

La Cour reconnaît qu'il peut y avoir de bonnes raisons pour garder secrète l'autorisation d'autoriser une surveillance secrète, en tout ou en partie, même après que la personne concernée ait pris connaissance de la mesure de surveillance. En effet, un accès complet à l'autorisation peut, dans certains cas, révéler les méthodes de la police ou des services secrets voire même rendre possible l'identification de leurs agents. En même temps, les informations contenues dans ces décisions peuvent être essentielles pour permettre à la personne concernée d'introduire une procédure pour contester la surveillance secrète. En conséquence, en matière de requête en divulgation d'une autorisation de surveillance secrète, les juridictions domestiques sont requises de garantir une mise en balance appropriée entre les intérêts de la personne surveillée et l'intérêt public. La personne surveillée doit avoir accès aux documents en question à moins qu'il n'existe des raisons impérieuses de s'opposer à cet accès²⁹.

6. *L'interception de conversations téléphoniques protégées par le secret professionnel*

L'article 8 offre une protection renforcée aux échanges entre les avocats et leurs clients, à défaut de quoi les avocats seraient incapables de défendre leurs clients s'ils étaient incapables de garantir la confidentialité de leurs échanges³⁰.

L'avocat doit, bien entendu, ne pas abuser du secret professionnel et la simple possibilité qu'il puisse en abuser est compensée par le besoin de respecter la confidentialité des relations entre l'avocat et son client³¹.

La loi doit déterminer clairement l'étendue du secret professionnel et dire comment et sous quelles conditions et par qui la différence doit être établie entre ce qui est protégé par le secret professionnel et ce qui ne l'est pas. Cette tâche ne peut pas être confiée à un membre de l'exécutif sans le contrôle d'un juge indépendant³².

Ensuite, les dispositions légales qui concernent l'examen, l'utilisation et la conservation des éléments ainsi obtenus, les précautions à prendre lors de la communication de ces éléments à d'autres parties, et les circonstances dans lesquelles les enregistrements peuvent ou doivent être effacés ou détruits, doivent offrir des garanties suffisantes pour la protection des éléments couverts par le secret professionnel obtenus dans le cadre d'une surveillance secrète. En particulier, le droit national doit déterminer avec suffisamment de clarté et de détail les procédures pour soumettre à une autorité de contrôle indépendante les affaires dans

²⁹ Cour eur. D.H., arrêt du 7 novembre 2017, n° 29431/05, *Zubkov et autres c. Russie*, § 129.

³⁰ Cour eur. D.H., arrêt du 15 juin 2017, n° 21979/08, *Oderovs c. Lettonie*, § 51; arrêt du 7 novembre 2017, n° 37717/05, *Dudchenko c. Russie*, § 104.

³¹ Cour eur. D.H., arrêt du 15 juin 2017, n° 21979/08, *Oderovs c. Lettonie*, § 51.

³² Cour eur. D.H., arrêt du 7 novembre 2017, n° 37717/05, *Dudchenko c. Russie*, § 106.

lesquelles des éléments couverts par le secret professionnel ont été obtenus dans le cadre de surveillances secrètes, les procédures pour assurer la destruction de ces éléments, les conditions sous lesquelles ces éléments peuvent être conservés et utilisés dans des procédures pénales et des investigations policières, et, dans ce cas, les procédures pour la conservation et la divulgation sécurisées de ces éléments et leur destruction ultérieure dès qu'ils ne sont plus nécessaires pour aucun des objectifs autorisés³³.

7. *La surveillance vidéo dans des auditorios universitaires*

La Cour a souligné le fait que les auditorios universitaires étaient des lieux de travail pour les enseignants. Mais que ce n'était pas seulement le lieu où ils enseignaient aux étudiants mais aussi un lieu où ils interagissaient avec eux; donc, ils développent des relations mutuelles et construisent leur identité sociale. Or, la surveillance vidéo secrète d'un employé sur son lieu de travail est une intrusion considérable dans sa vie privée. Et l'employeur ne peut pas réduire à néant la vie privée sociale des travailleurs sur les lieux du travail. Le droit au respect de la vie privée continue à exister même s'il peut être restreint dans la mesure de ce qui est nécessaire. En conséquence, la collecte de données par la surveillance vidéo concernait la vie privée des requérants³⁴.

Dans le cas d'espèce, les juridictions nationales n'ont pas vérifié la conformité des mesures de surveillance dès lors qu'elles n'ont pas considéré que la surveillance vidéo était constitutive d'une ingérence dans le droit au respect de la vie privée alors que l'agence de protection des données avait explicitement déclaré que la surveillance en question n'était pas conforme à la loi et, en particulier, à la loi sur la protection des données³⁵.

8. *La surveillance des communications dans le cadre des relations de travail*

La Grande Chambre a réformé l'arrêt *Barbulescu* du 12 janvier 2016³⁶ qui concernait l'utilisation à des fins privées d'un compte professionnel de messagerie instantanée Yahoo Messenger.

Tout d'abord, la Cour a relevé qu'il n'était pas certain que les règles restrictives de l'employeur aient laissé au requérant une attente raisonnable en matière de vie privée tout en indiquant que l'employeur ne pouvait pas réduire à néant l'exercice de la vie privée sociale sur le lieu du travail. Le respect de la vie privée et de la confidentialité des communications continue à s'imposer, même si ces dernières

³³ *Ibid.*, § 107.

³⁴ Cour eur. D.H., arrêt du 28 novembre 2017, n° 70838/13, *Antovic et Mirkovic c. Montenegro*, §§ 44-45, 55.

³⁵ *Ibid.*, §§ 56-57.

³⁶ Cour eur. D.H., arrêt du 12 janvier 2016, n° 61496/08, *Barbulescu c. Roumanie*.

peuvent être limitées dans la mesure de ce qui est nécessaire dans une société démocratique³⁷.

La Cour a estimé que les États contractants devaient se voir reconnaître une marge d'appréciation étendue pour évaluer la nécessité d'adopter un cadre juridique régissant les conditions dans lesquelles un employeur peut adopter une politique encadrant les communications non professionnelles, électroniques ou autres, de ses employés sur leur lieu de travail³⁸.

Néanmoins, la latitude dont jouissent les États dans ce domaine ne saurait être illimitée. Les juridictions internes doivent s'assurer que la mise en place par un employeur de mesures de surveillance de la correspondance et des autres communications (quelles qu'en soient l'étendue et la durée) s'accompagne de garanties adéquates et suffisantes contre les abus³⁹.

Tout en se disant consciente de la rapidité des évolutions dans ce domaine, la Cour estime toutefois que la proportionnalité et les garanties procédurales contre l'arbitraire sont des éléments essentiels. Dans ce contexte, les autorités nationales devraient tenir compte des facteurs suivants⁴⁰:

- 1° L'employé a-t-il été informé de la possibilité que l'employeur prenne des mesures de surveillance de sa correspondance et de ses autres communications ainsi que de la mise en place de telles mesures? Cette information peut être communiquée au personnel de diverses manières, en fonction des spécificités factuelles de chaque affaire. Toutefois, l'avertissement doit, en principe, être clair quant à la nature de la surveillance et préalable à la mise en place de celle-ci.
- 2° Quels ont été l'étendue de la surveillance opérée par l'employeur et le degré d'intrusion dans la vie privée de l'employé? Il faut distinguer entre la surveillance du flux des communications et celle de leur contenu. Il faut également prendre en compte les questions de savoir si la surveillance a ou non porté sur la totalité des communications et si elle a ou non été limitée dans le temps, ainsi que le nombre de personnes ayant eu accès aux résultats de la surveillance. Il faut aussi tenir compte des limites spatiales de la surveillance.
- 3° L'employeur a-t-il avancé des motifs légitimes pour justifier la surveillance de ces communications et l'accès à leur contenu même? La surveillance du contenu des communications requiert des justifications plus sérieuses étant nettement plus intrusive.
- 4° Aurait-il été possible de mettre en place un système de surveillance reposant sur des moyens et des mesures moins intrusifs que l'accès direct au contenu des communications de l'employé? Le point est de savoir si le but poursuivi

³⁷ Cour eur. D.H. (GC), arrêt du 5 septembre 2017, n° 61496/08, *Barbulescu c. Roumanie*, § 80.

³⁸ *Ibid.*, § 119.

³⁹ *Ibid.*, § 120.

⁴⁰ *Ibid.*, § 121.

par l'employeur pouvait être atteint sans que celui-ci n'accède directement et en intégralité au contenu des communications de l'employé.

5° Quelles ont été les conséquences de la surveillance pour l'employé qui en a fait l'objet ? De quelle manière l'employeur a-t-il utilisé les résultats de la mesure de surveillance, notamment ces résultats ont-ils été utilisés pour atteindre le but déclaré de la mesure ?

6° L'employé s'est-il vu offrir des garanties adéquates, notamment lorsque les mesures de surveillance de l'employeur avaient un caractère intrusif ? Ces garanties doivent notamment permettre d'empêcher que l'employeur n'ait accès au contenu même des communications en cause sans que l'employé n'ait été préalablement averti d'une telle éventualité.

Dans ce contexte, il est opportun de rappeler que pour pouvoir prospérer, les relations de travail doivent se fonder sur la confiance entre les personnes.

7° Enfin, les autorités internes devraient veiller à ce que les employés dont les communications ont été surveillées puissent bénéficier d'une voie de recours devant un organe juridictionnel ayant compétence pour statuer (du moins en substance) sur le respect des critères énoncés ci-dessus ainsi que sur la licéité des mesures contestées⁴¹.

Ceci étant, la Cour reconnaît que l'employeur a un intérêt légitime à assurer le bon fonctionnement de l'entreprise, ce qu'il peut faire en mettant en place des mécanismes lui permettant de vérifier que ses employés accomplissent leurs tâches professionnelles de manière adéquate et avec la célérité requise⁴².

En l'espèce, la Cour a reproché aux juridictions nationales d'avoir manqué, d'une part, de vérifier si le requérant avait été préalablement averti par son employeur de la possibilité que ses communications sur Yahoo Messenger puissent être surveillées et, d'autre part, de tenir compte du fait qu'il n'avait été informé ni de la nature ni de l'étendue de la surveillance dont il avait fait l'objet, ainsi que de ne pas avoir tenu compte du degré d'intrusion dans sa vie privée et sa correspondance. De surcroît, elle leur a reproché d'avoir failli à déterminer, premièrement, quelles raisons concrètes avaient justifié la mise en place des mesures de surveillance ; deuxièmement, si l'employeur aurait pu faire usage de mesures moins intrusives pour la vie privée et la correspondance du requérant et, troisièmement, si l'accès au contenu des communications avait été possible à son insu⁴³.

9. Le contrôle des mesures de surveillance secrète

L'examen et le contrôle des mesures de surveillance secrète peuvent intervenir à trois stades. D'abord lorsqu'on ordonne la surveillance, ensuite pendant qu'on la réalise et, enfin, après qu'elle ait cessé. Concernant les deux premières phases, la nature et la logique même de la surveillance secrète commandent d'exercer à l'insu

⁴¹ *Ibid.*, § 122.

⁴² *Ibid.*, § 127.

⁴³ *Ibid.*, § 140 (voy. aussi les opinions dissidentes).

de l'intéressé non seulement la surveillance comme telle, mais aussi le contrôle qui l'accompagne. Puisque l'on empêchera donc forcément l'intéressé d'introduire un recours effectif ou de prendre une part directe à un contrôle quelconque, il est indispensable que les procédures existantes procurent en elles-mêmes des garanties appropriées et équivalentes sauvegardant les droits de l'individu. De plus, il faut respecter aussi fidèlement que possible, dans les procédures de contrôle, les valeurs d'une société démocratique afin de ne pas dépasser les bornes de ce qui est nécessaire. En un domaine où les abus sont potentiellement si aisés dans des cas individuels et pourraient entraîner des conséquences préjudiciables pour la société démocratique tout entière, il est, en principe, souhaitable que le contrôle soit confié à un juge, car le pouvoir judiciaire offre les meilleures garanties d'indépendance, d'impartialité et de procédure régulière⁴⁴.

Quant au troisième stade, c'est-à-dire lorsque la surveillance a cessé, la question de la notification *a posteriori* des mesures de surveillance est indissolublement liée à celle de l'effectivité des recours judiciaires. La personne concernée ne peut guère, en principe, contester rétrospectivement devant la justice la légalité des mesures prises à son insu sauf si on l'avise de celles-ci⁴⁵. La Cour répète à cet égard qu'il peut ne pas être possible en pratique d'exiger une notification *a posteriori* dans tous les cas. L'activité ou le danger qu'un ensemble de mesures de surveillance vise à combattre peut subsister pendant des années, voire des décennies, après la levée de ces mesures. Une notification *a posteriori* à chaque individu touché par une mesure désormais levée risquerait de compromettre le but à long terme qui motivait à l'origine la surveillance. En outre, pareille notification risquerait de contribuer à révéler les méthodes de travail des services de renseignement, leurs champs d'activité et même, le cas échéant, l'identité de leurs agents. Cependant, il est souhaitable d'aviser la personne concernée après la levée des mesures de surveillance dès que la notification peut être donnée sans compromettre le but de la restriction⁴⁶.

Un recours judiciaire qui est dans l'incapacité d'examiner si l'ingérence contestée répond à un besoin social impérieux et est proportionnée aux objectifs poursuivis ne répond pas aux contraintes imposées par l'article 13 de la Convention⁴⁷.

10. *L'interdiction de communiquer durant une perquisition*

Conformément à la jurisprudence bien établie de la Cour, les appels téléphoniques réalisés depuis des locaux commerciaux aussi bien que depuis le domicile peuvent être couverts par les notions de vie privée et de correspondance⁴⁸. Dans le cas

⁴⁴ Cour eur. D.H., arrêt du 7 février 2017, n° 35285/08, *Irfan Güzel c. Turquie*, § 96; arrêt du 31 octobre 2017, n° 22767/08, *Dracos Ioan Rusu c. Roumanie*, § 39 (voy. la seconde opinion à propos de l'admissibilité des preuves obtenues de manière illégale).

⁴⁵ Cour eur. D.H., arrêt du 7 février 2017, n° 35285/08, *Irfan Güzel c. Turquie*, § 97.

⁴⁶ *Ibid.*, § 98.

⁴⁷ Cour eur. D.H., arrêt du 7 novembre 2017, n° 59589/10, *K. Moskalev c. Russie*, § 32.

⁴⁸ Cour eur. D.H., arrêt du 17 janvier 2017, n° 27153/07, *Cacuci, S.C. Virra & Cont Pad S.R.L. c. Roumanie*, § 65.

d'espèce, la Cour a considéré que l'interdiction faite à la personne concernée par la perquisition d'utiliser son téléphone portable durant celle-ci (et qui s'explique par le fait qu'il faut empêcher toute communication avec des personnes à l'extérieur, que ce soit par téléphone ou autrement), n'était pas une restriction qui dépassait ce qui était strictement nécessaire⁴⁹.

C. LES SAISIES DE DONNÉES ÉLECTRONIQUES

1. L'ingérence

La perquisition de locaux résidentiels et commerciaux, en ce compris la saisie d'équipements comprenant des données électroniques, constitue une ingérence dans la vie privée, le domicile et la correspondance des personnes concernées⁵⁰.

L'accès aux archives de l'ordinateur personnel du requérant et la condamnation qui s'en est ensuivie constituent une «ingérence des autorités publiques» dans le droit à la vie privée de l'intéressé⁵¹.

2. Le caractère nécessaire de l'ingérence dans une société démocratique

Une ingérence est considérée comme «nécessaire dans une société démocratique» pour atteindre un but légitime si elle répond à un «besoin social impérieux» et, en particulier, si elle est proportionnée au but légitime poursuivi et si les motifs invoqués par les autorités nationales pour la justifier apparaissent «pertinents et suffisants». S'il appartient aux autorités nationales de juger les premières si toutes ces conditions se trouvent remplies, c'est à la Cour qu'il revient de trancher en définitive la question de la nécessité de l'ingérence au regard des exigences de la Convention⁵².

Il faut aussi vérifier si la loi nationale offre des protections effectives contre les abus ou l'arbitraire, et, ensuite, si ces protections sont bien mises en œuvre en pratique⁵³.

Dans l'examen de la nécessité de l'ingérence, l'appréciation de l'existence de garanties adéquates et suffisantes contre les abus dépend de l'ensemble des circonstances de la cause, à savoir, par exemple, la nature, l'étendue et la durée des mesures éventuelles, les raisons requises pour les ordonner, les autorités compé-

⁴⁹ *Ibid.*, § 66.

⁵⁰ Cour eur. D.H., arrêt du 19 janvier 2017, n° 63638/14, *Posevini c. Bulgarie*, § 65.

⁵¹ Cour eur. D.H., arrêt du 30 mai 2017, n° 32600/12, *Trabajo Rueda c. Espagne*, § 32 (voy. le § 33 et s. pour la question de la prévisibilité de l'ingérence par la loi et le but légitime poursuivi).

⁵² Cour eur. D.H., arrêt du 30 mai 2017, n° 32600/12, *Trabajo Rueda c. Espagne*, § 42.

⁵³ Cour eur. D.H., arrêt du 19 janvier 2017, n° 63638/14, *Posevini c. Bulgarie*, § 69.

tentes pour les permettre, exécuter et contrôler, et le type de recours fourni par le droit interne⁵⁴.

Le fait que la perquisition se base sur un mandat judiciaire ne constitue pas nécessairement une protection suffisante. Il faut, en outre, vérifier si le contrôle judiciaire préalable a été correctement réalisé. Ceci signifie que le juge doit correctement examiner l'existence d'un soupçon raisonnable qui justifie la perquisition et rédiger le mandat de perquisition de manière à maintenir celle-ci dans des limites raisonnables. Enfin le juge doit être convaincu que la perquisition est de nature à fournir des preuves pertinentes⁵⁵.

En présence d'un contrôle judiciaire préalable, l'absence d'une procédure permettant de contester *a posteriori* les perquisitions ne les rend pas disproportionnées⁵⁶.

Quant à la nécessité de l'ingérence dans une société démocratique, à défaut de pouvoir prévenir la saisie de documents étrangers à l'objet de l'enquête et *a fortiori* de ceux relevant de la confidentialité qui s'attache aux relations entre un avocat et son client, les personnes concernées devaient pouvoir contester *a posteriori*, de manière concrète et effective, la régularité de leur saisie. Il appartient, dès lors, au juge saisi d'allégations motivées selon lesquelles des documents précisément identifiés auraient été appréhendés alors qu'ils étaient sans lien avec l'enquête ou qu'ils relevaient de la confidentialité qui s'attache aux relations entre un avocat et son client, de statuer sur leur sort au terme d'un contrôle concret de proportionnalité et d'ordonner, le cas échéant, leur restitution⁵⁷.

La Cour observe que, loin de se limiter à vérifier la véracité des faits portés à sa connaissance en accédant au dossier « mes documents », la police a procédé à une inspection de l'intégralité du contenu des archives de l'ordinateur en ouvrant et en examinant également le fichier « Incoming » du programme eMule, le tout sans avoir recueilli au préalable l'autorisation judiciaire requise – ce qui n'aurait été justifié, le cas échéant, que par une « nécessité urgente »⁵⁸.

Aux yeux de la Cour, il est difficile d'apprécier, en l'espèce, l'urgence qui aurait contraint la police à saisir les archives de l'ordinateur personnel du requérant et à accéder à leur contenu, sans obtenir au préalable l'autorisation judiciaire normalement requise. En effet, il n'existait aucun risque de disparition de fichiers puisqu'il s'agissait d'un ordinateur saisi et retenu par la police et non connecté au réseau Internet. La Cour ne parvient pas à déceler les raisons pour lesquelles l'attente d'une autorisation judiciaire préalable à l'intervention sur l'ordinateur du requé-

⁵⁴ Cour eur. D.H., arrêt du 30 mai 2017, n° 32600/12, *Trabajo Rueda c. Espagne*, § 43.

⁵⁵ Cour eur. D.H., arrêt du 19 janvier 2017, n° 63638/14, *Posevini c. Bulgarie*, § 70.

⁵⁶ *Ibid.*, § 73. Par contre, la Cour a considéré qu'il y avait violation de l'article 13 de la Convention à ce titre.

⁵⁷ Cour eur. D.H., décision du 21 mars 2017, n° 33931/12, *Janssen Cilag S.A.S. c. France*, § 19.

⁵⁸ Cour eur. D.H., arrêt du 30 mai 2017, n° 32600/12, *Trabajo Rueda c. Espagne*, § 45.

rant, qui pouvait être obtenue relativement rapidement, aurait entravé l'enquête menée par la police sur les faits dénoncés⁵⁹.

D. LA PROTECTION CONTRE LA DIVULGATION DE DONNÉES

1. *La divulgation de relevés téléphoniques*

Les appels téléphoniques reçus dans des locaux privés sont compris dans les notions de vie privée et de correspondance. L'exploitation d'informations se rapportant à des conversations téléphoniques, notamment les dates et durées de celles-ci ainsi que les numéros composés, peut poser problème au regard de l'article 8 de la Convention, ces éléments faisant partie intégrante des communications téléphoniques. Ainsi, pareilles informations s'analysent en des données à caractère personnel⁶⁰.

En l'espèce, la Cour a estimé que la divulgation, sans le consentement de la requérante, des données à caractère personnel se rapportant aux services de téléphonie fixe fournis à celle-ci ainsi que leur utilisation à son encontre dans le cadre d'une procédure civile, ont constitué une ingérence dans l'exercice de son droit au respect de la vie privée et de la correspondance⁶¹.

2. *La divulgation des collaborateurs dans les anciens pays de l'Est (le phénomène de la Lustration)*

a. La divulgation de l'affiliation aux services de sécurité antérieurs

La publication d'informations systématiquement collectées et conservées par les autorités publiques (peu importe si elles concernent des activités privées ou publiques d'un individu), tombe dans le champ de l'article 8 et constitue une ingérence dans le droit au respect de la vie privée⁶².

Dénoncer les membres du personnel et les collaborateurs secrets de l'appareil répressif du régime communiste et qui ont travaillé ou qui continuent à travailler à des postes-clés du secteur public ou privé depuis la chute de ces régimes, vise à améliorer la transparence de la vie publique et à promouvoir la confiance dans les nouvelles institutions démocratiques. Cela permet aussi à la société bulgare de prendre connaissance des détails de son passé récent. Ce sont autant d'objectifs légitimes⁶³.

La réponse à la question de savoir si l'ingérence était nécessaire dans une société démocratique ne consiste pas à savoir si on aurait pu mettre en place des règles

⁵⁹ *Ibid.*, § 46.

⁶⁰ Cour eur. D.H., arrêt du 28 mars 2017, n° 33074/04, *Savotchko c. République de Moldavie*, § 29.

⁶¹ *Ibid.*, § 30.

⁶² Cour eur. D.H., décision du 5 décembre 2017, n° 38334/08 et 68242/16, *H.B. Anchev c. Bulgarie*, § 92.

⁶³ *Ibid.*, § 100.

moins intrusives ou si ces objectifs auraient pu être atteints d'une autre façon. Il s'agit plutôt ici de savoir si les autorités bulgares ont bien agi dans les limites de leur marge d'appréciation⁶⁴.

Les États membres qui ont succédé à des régimes non démocratiques disposent d'une large marge d'appréciation dans le choix dans la manière de gérer l'héritage des régimes antérieurs. Leurs autorités disposent d'une légitimité démocratique directe et une meilleure connaissance de l'expérience historique et politique de leur pays ; elles sont donc mieux placées que la Cour pour décider les mesures transitoires requises dans l'intérêt public⁶⁵.

Comme les autres ex-États communistes de l'Europe de l'Est, la Bulgarie a dû mettre en place des mesures pour gérer l'héritage de son régime communiste en ce compris de son appareil répressif. Comme la Cour l'a déjà relevé, ces États n'ont pas tous agi de la même façon. Certains ont décidé d'interdire à ces individus ou à ceux qui parmi eux ont tenté de cacher leurs activités passées, de travailler dans le secteur public voire même dans certains cas dans le secteur privé. D'autres ont réduit leur pension. D'autres les ont déchus de leurs droits. D'autres encore les ont enregistrés et ceux qui ne reconnaissaient pas volontairement leurs activités passées étaient dénoncés. En Bulgarie, il a finalement été décidé de mettre en place un système de divulgation de l'affiliation aux services de sécurité antérieurs⁶⁶.

Les autorités bulgares disposent d'une large marge d'appréciation également en raison du fait que la législation a été méticuleusement passée en revue par la Cour constitutionnelle en tenant compte de la nécessité de mettre en balance les intérêts conflictuels en jeu⁶⁷. De plus, le choix opéré par les autorités bulgares n'était pas situé aux limites de leur marge d'appréciation⁶⁸.

b. La publication d'une décision non définitive

La publication de la décision de la commission de vérification des faits considérant que le requérant avait collaboré avec les services de sécurité du régime précédent et qu'il remplissait par conséquent les critères pour que sa candidature ou l'exercice d'une fonction publique soit restreint, sur le site Web de la commission, représente une ingérence dans son droit au respect de la vie privée. La Cour a relevé que la publication de cette décision avait accru son effet sur le droit au respect de la vie privée du requérant⁶⁹.

⁶⁴ *Ibid.*, § 101.

⁶⁵ *Ibid.*, § 102.

⁶⁶ *Ibid.*, § 103.

⁶⁷ *Ibid.*, § 104.

⁶⁸ *Ibid.*, § 105 (voy. le détail aux §§ 106 et s.).

⁶⁹ Cour eur. D.H., arrêt du 6 avril 2017, n° 2229/15, *Karajanov c. L'ancienne République yougoslave de Macédoine*, §§ 71-72.

En l'espèce, la Cour a considéré que la publication de cette décision à l'effet de garantir une plus grande transparence, l'accès du public aux documents contenus dans le dossier du requérant et le contrôle public du processus décisionnel de la commission, ne correspondait à aucun des objectifs légitimes visés à l'article 8, § 2, de la Convention. De plus, la Cour a considéré que la divulgation d'une décision non définitive était inconciliable avec les objectifs généraux de la lustration que la Cour a acceptée comme étant légitime. À cet égard, la Cour a retenu que le requérant était âgé de 77 ans lorsque la commission avait prononcé sa décision et qu'il n'exerçait aucune fonction publique. De plus, il n'était pas soutenu qu'il était candidat à une quelconque fonction publique. Ce n'est pas pour autant que la publication de la décision définitive serait légitime⁷⁰.

E. LA PROTECTION DES DONNÉES RELATIVES À LA SANTÉ

1. *L'importance de la protection des données et de celles relatives à la santé*

La notion de vie privée comprend des éléments tels que les informations personnelles relatives à un patient⁷¹. La Cour a répété que la protection des données à caractère personnel (et dont les données médicales ne sont pas les moindres), était d'une importance fondamentale pour l'exercice du droit au respect de la vie privée. Le respect de la confidentialité des informations relatives à la santé est un principe vital de tous les systèmes juridiques des États membres. Ces considérations sont d'autant plus fortes lorsqu'elles concernent la protection de la confidentialité de la séropositivité d'une personne⁷².

2. *Utilisation de données et ingérence*

La conservation systématique et toute autre utilisation d'informations relatives à la vie privée d'un individu par des autorités publiques constituent des ingérences dans son droit au respect de la vie privée. Ceci est d'autant plus vrai lorsque l'information concerne le passé distant d'une personne ou lorsque le traitement concerne des catégories d'informations hautement intimes et sensibles, en particulier les informations relatives à la santé physique ou mentale d'un individu identifiable⁷³.

3. *Le caractère nécessaire de l'ingérence en matière de protection des données et de données relatives à la santé*

À propos de la nécessité de l'ingérence dans une société démocratique, la Cour a noté que, en tenant compte de l'importance fondamentale de la protection des

⁷⁰ *Ibid.*, § 75.

⁷¹ Cour eur. D.H., arrêt du 12 décembre 2017, n° 7653/06, *M.M. c. Russie*, § 61.

⁷² *Ibid.*, § 65.

⁷³ Cour eur. D.H., arrêt du 26 janvier 2017, n° 42788/06, *Surikov c. Ukraine*, § 70.

données pour un exercice effectif du droit au respect de la vie privée, la marge d'appréciation reconnue aux États membres dans la définition de leur cadre législatif et réglementaire respectif dans cette matière est plutôt limitée. En ce sens, la question de la nécessité de l'ingérence peut recouvrir la question qui concerne la qualité des garanties procédurales requises qui sont offertes dans la loi nationale de l'État membre⁷⁴.

À ce jour il existe un certain niveau de consensus au niveau international et en particulier entre les États membres du Conseil de l'Europe en ce qui concerne les principes fondamentaux de la protection des données et les garanties procédurales de base correspondantes qui doivent être reprises dans les cadres législatifs nationaux afin de justifier la nécessité de toute ingérence possible. En particulier la Cour a déjà affirmé que :

- 1° le droit national des États membres devait notamment garantir que des données à caractère personnel en question devaient être pertinentes et non excessives au regard des finalités pour lesquelles elles avaient été collectées ou conservées ;
- 2° les données devaient être conservées dans une forme qui ne permette pas l'identification de la personne concernée plus longtemps que ce qui n'est requis pour la finalité pour laquelle ces données sont conservées ;
- 3° et que les données conservées doivent être efficacement protégées contre tout abus et mauvaise utilisation.

La Cour a aussi rappelé qu'il était essentiel pour le droit applicable de fournir des règles claires et détaillées pour déterminer l'étendue et la mise en œuvre des mesures pertinentes aussi bien que les garanties minimales concernant entre autres la durée, la conservation, l'utilisation, l'accès par des parties tierces, les procédures visant à assurer l'intégrité et la confidentialité des données et les procédures pour leur destruction. Le droit applicable doit fournir des garanties suffisantes contre le risque d'abus et d'arbitraire à chaque étape du traitement des données. Il y a plusieurs moments importants auxquels des questions relatives à la protection des données peuvent apparaître au regard de l'article 8 en ce compris durant la collecte, la conservation, l'utilisation et la communication de données. À chaque étape, des garanties appropriées et adéquates qui doivent refléter les principes repris dans les instruments applicables en matière de protection des données doivent être mises en place afin de justifier la nécessité de l'ingérence au regard de l'article 8⁷⁵.

En l'espèce, l'information selon laquelle le requérant souffrait d'une maladie mentale représente par sa seule nature une donnée à caractère personnel hautement sensible, peu importe si ces données étaient indicatives d'un diagnostic médical particulier. La collecte, la conservation, la divulgation et tout autre type

⁷⁴ *Ibid.*, § 73.

⁷⁵ *Ibid.*, § 74.

de traitement d'une telle information tombent par conséquent dans la sphère de l'article 8⁷⁶.

La Cour répète que les principes fondamentaux de la protection des données requièrent que la conservation de données doit être proportionnée au regard de la finalité de la collecte de ces données et qu'il faut limiter les durées de conservation. En ce sens, la Cour considère que déléguer à chaque employeur une fonction publique qui comprend la conservation de données sensibles relatives à la santé de leurs employés ne peut se justifier au regard de l'article 8 que si pareille conservation est accompagnée par des garanties procédurales particulièrement sévères pour garantir notamment que de telles données resteront strictement confidentielles, ne seront pas utilisées pour d'autres motifs que ceux pour lesquels ces données ont été collectées, et que ces données seront mises à jour⁷⁷.

Dans la mesure où le droit applicable tel qu'interprété et appliqué par les juridictions nationales dans le cas d'espèce, autorise la conservation des données relatives à la santé du requérant pour une période très longue et qu'il autorise leur divulgation et leur utilisation pour des finalités sans lien avec la finalité pour laquelle elles ont été collectées à l'origine, la Cour considère qu'une habilitation aussi large représente une ingérence disproportionnée dans le droit au respect de la vie privée du requérant. Elle ne peut pas être vue comme étant nécessaire dans une société démocratique⁷⁸.

F. LA PROTECTION DES DONNÉES BIOMÉTRIQUES

1. *L'ingérence dans l'exercice du droit au respect de la vie privée*

Le simple fait de mémoriser des données relatives à la vie privée d'un individu constitue une ingérence au sens de l'article 8. Peu importe que les informations mémorisées soient ou non utilisées par la suite. Quant aux profils ADN, ils contiennent une quantité importante de données à caractère personnel unique⁷⁹. La conservation d'échantillons cellulaires d'ADN et de profils ADN constitue donc une ingérence dans le droit à la vie privée. Le tout est de savoir si cette ingérence est justifiée⁸⁰.

2. *Le but légitime poursuivi par l'ingérence*

La Cour a précisé qu'elle avait pleinement conscience que, pour protéger leur population comme elles en ont le devoir, les autorités nationales étaient amenées à constituer des fichiers contribuant efficacement à la répression et à la préven-

⁷⁶ *Ibid.*, § 75.

⁷⁷ *Ibid.*, § 86.

⁷⁸ *Ibid.*, § 89.

⁷⁹ Cour eur. D.H., arrêt du 22 juin 2017, n° 8806/12, *Aycaguer c. France*, § 33.

⁸⁰ Cour eur. D.H., décision du 25 avril 2017, n° 24344/08, *Paul Karl Thomas c. Royaume-Uni*, § 29.

tion de certaines infractions, notamment les plus graves, comme celles de nature sexuelle pour lesquelles le FNAEG a été créé. Toutefois, de tels dispositifs ne sauraient être mis en œuvre dans une logique excessive de maximalisation des informations qui y sont placées et de la durée de leur conservation. En effet, sans le respect d'une nécessaire proportionnalité au regard des objectifs légitimes qui leur sont attribués, les avantages qu'ils apportent seraient obérés par les atteintes graves qu'ils causeraient aux droits et libertés que les États doivent assurer en vertu de la Convention aux personnes placées sous leur juridiction⁸¹.

3. *La nécessité de l'ingérence*

La protection des données à caractère personnel joue un rôle fondamental dans l'exercice du droit au respect de la vie privée. La législation interne doit donc ménager des garanties appropriées pour empêcher toute utilisation de données à caractère personnel qui ne serait pas conforme aux garanties prévues par cet article.

La nécessité de disposer de telles garanties se fait d'autant plus sentir lorsqu'il s'agit de protéger les données à caractère personnel soumises à un traitement automatique, en particulier lorsque ces données sont utilisées à des fins policières.

Le droit interne doit notamment assurer que ces données soient pertinentes et non excessives par rapport aux finalités pour lesquelles elles sont enregistrées, et qu'elles soient conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles ont été enregistrées.

Le droit interne doit aussi contenir des garanties aptes à protéger efficacement les données à caractère personnel enregistrées contre les usages impropres et abusifs, tout en offrant une possibilité concrète de présenter une requête en effacement des données mémorisées⁸².

4. *La durée de conservation*

Dans le cas du FNAEG, la Cour a noté que la durée de conservation ne variait pas en fonction de la nature et de la gravité de l'infraction commise⁸³.

S'agissant de la procédure d'effacement, celle-ci n'existait que pour les personnes soupçonnées, et non pour celles qui avaient été condamnées. Or, la Cour estime que les personnes condamnées devraient également se voir offrir une possibilité concrète de présenter une requête en effacement des données mémorisées et

⁸¹ Cour eur. D.H., arrêt du 22 juin 2017, n° 8806/12, *Aycaguer c. France*, § 34.

⁸² *Ibid.*, § 38.

⁸³ *Ibid.*, § 45.

ce, comme elle l'a rappelé précédemment, afin que la durée de conservation soit proportionnée à la nature des infractions et aux buts des ingérences⁸⁴.

En conséquence, le régime actuel de conservation des profils ADN dans le FNAEG n'offre pas, en raison tant de sa durée que de l'absence de possibilité d'effacement, une protection suffisante aux personnes concernées. Elle ne traduit donc pas un juste équilibre entre les intérêts publics et privés concurrents en jeu⁸⁵.

G. LA PROTECTION DES DONNÉES BANCAIRES

1. *L'ingérence dans l'exercice du droit au respect de la vie privée*

La collecte, la conservation et le fait de rendre disponibles les transactions bancaires professionnelles constituent une ingérence dans le droit au respect du secret professionnel et de la vie privée du requérant⁸⁶.

2. *La prévisibilité de l'ingérence*

Il ne suffit pas que l'ingérence en question ait une base en droit national. Il faut, en outre, que la loi soit accessible aux personnes concernées et prévisible quant à ses effets⁸⁷.

Dans le contexte d'une collecte secrète d'informations, il est essentiel d'avoir des règles claires et détaillées qui gouvernent l'étendue et la mise en œuvre des mesures aussi bien que les protections minimales concernant entre autres la durée, la conservation, l'utilisation, l'accès par des tiers, les procédures pour préserver l'intégrité et la confidentialité des données et des procédures pour leur destruction, afin de fournir des garanties suffisantes contre les risques d'abus et d'arbitraire. En l'espèce, ces questions importantes sont intimement liées à la question plus large de savoir si l'ingérence était nécessaire dans une société démocratique⁸⁸.

3. *Le caractère nécessaire de l'ingérence dans une société démocratique*

L'ingérence doit correspondre à un besoin social impérieux et, en particulier, que l'ingérence soit proportionnée à l'objectif légitime poursuivi. Les États membres disposent d'une certaine marge d'appréciation dans l'évaluation de la nécessité de l'ingérence mais cela va de pair avec un contrôle européen qui recouvre tant la législation que les décisions qui l'appliquent. Les finalités visées à l'article 8, § 2,

⁸⁴ *Ibid.*, § 44.

⁸⁵ *Ibid.*, § 33.

⁸⁶ Cour eur. D.H., arrêt du 27 avril 2017, n° 73607/13, *Sommer c. Allemagne*, § 48.

⁸⁷ *Ibid.*, § 50.

⁸⁸ *Ibid.*, § 53.

doivent être interprétées de manière étroite et le besoin d'y recourir dans un cas d'espèce doit être établi de manière convaincante⁸⁹.

La Cour doit être convaincue qu'il existe des garanties suffisantes et appropriées contre l'arbitraire, en ce compris la possibilité d'un contrôle effectif de la mesure en cause. De plus, la Cour a déjà reconnu l'importance de garanties procédurales spécifiques quand il s'agit de protéger la confidentialité des échanges entre un avocat et son client. À condition de faire l'objet d'un contrôle strict, il est possible d'imposer certaines obligations aux avocats concernant leurs relations avec leurs clients, par exemple dans le cas où il existe des preuves plausibles de l'implication de l'avocat dans un crime et dans le cadre de la lutte contre le blanchiment d'argent. La Convention n'empêche pas le droit national d'autoriser les perquisitions dans les bureaux d'avocats pour autant que des garanties appropriées soient prévues comme, par exemple, la présence d'un représentant du barreau⁹⁰.

En l'espèce, les requêtes d'informations du parquet étaient limitées seulement en ce qui concerne la période concernée mais autrement elles concernaient toutes les informations relatives au compte bancaire et aux transactions bancaires du requérant. En conséquence, la Cour doit examiner si les manquements dans la limitation des requêtes d'informations étaient contrebalancés par des garanties procédurales suffisantes capables de protéger le requérant contre tout abus ou arbitraire⁹¹.

Dans la mesure où les requêtes du parquet indiquaient qu'à défaut pour la banque de fournir volontairement l'information elle recevrait des convocations contraignantes pour un interrogatoire formel, la Cour doute que la banque ait agi de manière totalement volontaire. De plus, la Cour a répété que la conservation ou la collecte d'informations relatives à la vie privée d'un individu constituait une ingérence au sens de l'article 8 peu importe qui était le propriétaire du média qui contenait les informations recherchées⁹².

H. LA PROTECTION DES DONNÉES FISCALES

1. *Les droits en conflit*

Les données collectées et traitées par les sociétés requérantes et publiées par elles dans le journal *Veropörssi*, qui donnait des précisions sur les revenus imposables provenant du travail et d'autres sources, ainsi que du patrimoine net imposable de nombreuses personnes, relèvent clairement de la vie privée de celles-ci, indé-

⁸⁹ *Ibid.*, § 55.

⁹⁰ *Ibid.*, § 56.

⁹¹ *Ibid.*, § 57.

⁹² *Ibid.*, § 59.

pendamment du fait que, en vertu du droit finlandais, le public avait la possibilité d'accéder à ces données suivant certaines règles⁹³.

Par ailleurs, la décision de la Commission de protection des données (interdisant de poursuivre la diffusion des données de la façon litigieuse), entérinée par les juridictions nationales, a entraîné une ingérence dans l'exercice par les sociétés requérantes du droit de communiquer des idées tel que celui-ci est garanti par l'article 10 de la Convention⁹⁴.

2. Sur la prévisibilité de l'ingérence

La Cour a jugé qu'il ressortait de manière raisonnablement claire du libellé et des travaux préparatoires de la loi qu'il était possible que les autorités nationales concluent à un moment ou à un autre, ainsi qu'elles l'ont fait en l'espèce, qu'une base de données établie à des fins de journalisme ne pouvait pas être diffusée telle quelle. La quantité et la forme des données publiées ne pouvaient pas excéder la portée de la dérogation et celle-ci, de par sa nature même, devait être interprétée de manière restrictive, ainsi que la C.J.U.E. l'a clairement indiqué⁹⁵.

De plus, les sociétés requérantes étaient des entreprises de médias et, en cette qualité, auraient dû avoir conscience que la collecte et la diffusion à grande échelle des données en cause (qui concernaient environ un tiers des contribuables finlandais ou 1,2 million de personnes, soit un nombre dix à vingt fois supérieur au nombre de données divulguées par les autres médias à l'époque des faits), pouvaient ne pas être considérées comme un traitement de données effectué aux « seules » fins de journalisme au regard de la loi finlandaise ou de la réglementation de l'Union européenne⁹⁶.

En l'espèce, à la suite de la commande de données fiscales effectuée par les sociétés requérantes auprès de la direction générale des impôts en 2000 et 2001, le médiateur chargé de la protection des données avait invité les intéressées à fournir d'autres informations concernant leurs commandes et leur avait indiqué que les données ne pourraient pas être divulguées si le magazine *Veropörssi* continuait de paraître sous sa forme habituelle. Or, au lieu de se conformer à la demande d'information du médiateur, les sociétés requérantes ont contourné la voie ordinairement suivie par les journalistes pour accéder aux données recherchées et se sont organisées pour que celles-ci soient collectées manuellement dans les centres locaux des impôts. Cette attitude est de nature à donner à penser qu'elles s'attendaient à rencontrer des difficultés pour invoquer la dérogation à des fins de journalisme et la législation nationale pertinente sur l'accès aux données fiscales⁹⁷.

⁹³ Cour eur. D.H. (GC), arrêt du 27 juin 2017, n° 931/13, *Satakunnan Markkinapörssi Oy et Satamedia Oy c. Finlande*, § 138.

⁹⁴ *Ibid.*, § 140.

⁹⁵ *Ibid.*, § 149.

⁹⁶ *Ibid.*, § 151.

⁹⁷ *Ibid.*, § 152.

De plus, la version de 1992 des lignes directrices à l'intention des journalistes (mises à jour en 2005, 2011 et 2014) indiquait expressément que les principes en matière de protection des personnes s'appliquaient également à l'utilisation d'informations figurant dans des documents publics ou d'autres sources publiques, et que le fait de mettre des informations à la disposition du public ne signifiait pas nécessairement que ces informations pouvaient être librement publiées. Les sociétés requérantes avaient certainement connaissance de ces lignes directrices, élaborées à des fins d'autorégulation par les journalistes et éditeurs finlandais⁹⁸.

À la lumière des considérations qui précèdent, la Cour en a conclu que l'ingérence litigieuse dans l'exercice par les sociétés requérantes de leur droit à la liberté d'expression était « prévue par la loi »⁹⁹.

3. Sur le but légitime par l'ingérence

Le médiateur chargé de la protection des données a agi sur le fondement de plaintes concrètes d'individus alléguant que la publication de données fiscales dans le magazine *Veropörssi* avait porté atteinte à leur droit à la vie privée. Ainsi que le montrent clairement les chiffres, les pratiques de publication des sociétés requérantes ciblaient un groupe très important de personnes physiques assujetties à l'impôt en Finlande. On peut raisonnablement considérer que l'ensemble des contribuables finlandais ont été lésés, directement ou indirectement, par l'activité de publication des sociétés requérantes, étant donné que les lecteurs étaient en mesure d'évaluer les revenus imposables de tout contribuable simplement en regardant si son nom figurait ou non dans les listes publiées par le magazine *Veropörssi*¹⁰⁰.

Indépendamment de la question de savoir s'il était nécessaire d'identifier chacun des plaignants au niveau national, la Cour a estimé que l'argument des sociétés requérantes ne tenait pas compte de la nature et de la portée des obligations des autorités nationales chargées de la protection des données en application. Concernant celles-ci, il convient de noter que, selon la C.J.U.E., la garantie d'indépendance des autorités nationales de contrôle a été établie en vue de renforcer la protection des personnes et des organismes qui sont concernés par leurs décisions. Pour garantir cette protection, les autorités nationales de contrôle doivent, notamment, assurer un juste équilibre entre, d'une part, le respect du droit fondamental à la vie privée et, d'autre part, les intérêts qui commandent une libre circulation des données à caractère personnel. La protection de la vie privée était donc au cœur de la législation relative à la protection des données que ces autorités avaient mandat de faire respecter¹⁰¹.

⁹⁸ *Ibid.*, § 153.

⁹⁹ *Ibid.*, § 154.

¹⁰⁰ *Ibid.*, § 157.

¹⁰¹ *Ibid.*, § 158.

À la lumière des considérations qui précèdent et eu égard aux buts de la Convention sur la protection des données, qui a inspiré la directive 95/46 et, plus récemment, le règlement 2016/79 (RGPD), l'ingérence dans l'exercice par les sociétés requérantes de leur droit à la liberté d'expression poursuivait à l'évidence le but légitime de « la protection de la réputation ou des droits d'autrui » au sens de l'article 10, § 2¹⁰².

I. LE DROIT D'ACCÈS AUX DONNÉES

En ce qui concerne l'accès aux données personnelles détenues par des autorités publiques (à l'exception des informations relatives à des considérations de sécurité nationale), la Cour a répété l'existence d'un intérêt vital protégé par l'article 8 dans le chef des personnes désirant recevoir les informations nécessaires pour connaître et comprendre leur enfance et le début de leur formation ou pour retrouver leurs origines (en particulier, l'identité de leurs parents naturels), les informations concernant les risques sanitaires auxquels ces personnes ont été exposées, ou les informations relatives aux dossiers créés par les services secrets durant un régime totalitaire¹⁰³.

Dans toutes ces hypothèses, la Cour a jugé que l'obligation positive à charge de l'État membre l'obligeait à fournir une procédure effective et accessible permettant aux requérants d'avoir accès à toutes les informations pertinentes et appropriées nécessaires pour ces finalités¹⁰⁴.

Dans le cas d'espèce où le requérant souhaitait obtenir accès à son dossier personnel au ministère de l'intérieur et en particulier à son évaluation psychologique réalisée lorsqu'il avait postulé pour participer à une mission internationale de police, la Cour a considéré que, dans ces circonstances, l'accès aux informations relatives aux raisons pour lesquelles il avait été considéré inapte à participer à cette mission internationale, spécialement en ce que cela résultait de l'évaluation psychologique, devait être considéré comme suffisamment étroitement lié à sa vie privée au sens de l'article 8 que pour poser problème au regard de cette disposition¹⁰⁵.

J. LES LISTES NOIRES DE TRAVAILLEURS SYNDIQUÉS DANS LE BÂTIMENT

Bien que l'objet de l'article 8 soit essentiellement de protéger les individus contre les ingérences arbitraires par des autorités publiques, il ne se contente pas d'imposer à l'État de s'abstenir de pareille ingérence. Il peut, en outre, y avoir des obligations positives inhérentes à un respect effectif de la vie privée ou familiale.

¹⁰² *Ibid.*, § 159 (voy. les opinions dissidentes).

¹⁰³ Cour eur. D.H., arrêt du 7 décembre 2017, n° 12504/09, *Yonchev c. Bulgarie*, § 49.

¹⁰⁴ *Ibid.*, § 50.

¹⁰⁵ *Ibid.*, § 46.

Ces obligations peuvent comprendre l'adoption de mesures destinées à garantir le respect de la vie privée même dans la sphère des relations des individus entre eux. Le choix des moyens destinés à garantir la conformité avec l'article 8 dans la sphère de relations des individus entre eux est, en principe, une décision qui relève de la marge d'appréciation des États membres. Il existe plusieurs façons de garantir le respect de la vie privée et la nature de l'obligation de l'État dépendra de l'aspect de la vie privée qui est en l'espèce en cause¹⁰⁶.

En l'espèce, l'État a mis en œuvre cette obligation positive en partie en incriminant la conservation illégale de données relatives à l'affiliation syndicale et aux activités syndicales¹⁰⁷. Il a également légiféré pour permettre l'introduction d'un recours civil. Dans le cadre des recours qui furent introduits, les entreprises ont reconnu que les données étaient confidentielles et n'auraient pas dû être utilisées. Elles ont également payé des indemnités aux requérants et aux autres pour la conservation illégale de ces données ainsi que pour leur utilisation¹⁰⁸. Au vu de ce qui précède et en tenant compte du fait que ce sont des actions d'entreprises privées qui sont en cause plutôt que des actions des autorités nationales, la Cour a considéré que le cadre juridique fournissait une combinaison de recours domestiques qui se sont avérés effectifs et appropriés et qui ont abouti à la reconnaissance de la violation des droits du requérant¹⁰⁹.

K. LES LITIGES EN MATIÈRE DE FILIATION

1. *Les contestations de paternité*

La tentative par un père présumé de contester officiellement sa paternité concerne sa vie privée. De la même façon, cela concerne la vie privée et familiale de la mère et de l'enfant¹¹⁰.

Le refus de rouvrir une action en contestation de paternité constitue une ingérence dans le droit au respect de la vie privée et familiale des pères ou doit être vu comme un manquement reproché dans le chef de l'État de se conformer à une obligation positive à sa charge¹¹¹.

L'introduction d'un délai ou de toute autre limitation en matière de procédure de paternité peut être justifiée par le souhait de garantir la sécurité juridique dans les relations familiales et protéger les intérêts de l'enfant¹¹².

¹⁰⁶ Cour eur. D.H., décision du 28 mars 2017, n° 54357/15, *David Smith c. Royaume-Uni*, § 37.

¹⁰⁷ *Ibid.*, § 38.

¹⁰⁸ *Ibid.*, § 39.

¹⁰⁹ *Ibid.*, § 40. En ce qui concerne le blacklisting du requérant en raison de son affiliation à un syndicat et l'application de l'article 35, § 3, b, de la Convention, voy. le § 42 et s.

¹¹⁰ Cour eur. D.H., arrêt du 7 mars 2017, n° 52629/11, *R.L et autres c. Danemark*, § 38.

¹¹¹ *Ibid.*, § 39.

¹¹² Cour eur. D.H., arrêt du 7 mars 2017, n° 52629/11, *R.L et autres c. Danemark*, § 40; décision du 17 octobre 2017, n° 54056/15, *Tadeusz Kordek c. Pologne*, § 27.

Il demeure néanmoins à vérifier si les autorités ont atteint un juste équilibre entre l'intérêt général à la protection de la sécurité juridique dans les relations familiales et l'intérêt du requérant à contester sa paternité au vu de la réalité biologique¹¹³.

2. *Les actions en recherche de paternité – Le droit à établir les détails de son identité*

Les procédures en recherche de paternité tombent dans le champ de l'article 8. La naissance et, en particulier, les circonstances dans lesquelles un enfant est né, font partie de la vie privée de l'enfant et des adultes concernés. Le respect de la vie privée requiert que chacun doit pouvoir être capable d'établir les détails de son identité. Ceci comprend l'obtention des informations nécessaires pour découvrir la vérité concernant certains aspects importants de l'identité personnelle telle que l'identité de ses parents¹¹⁴.

D'un côté, les individus ont le droit de connaître leur identité et de l'autre côté, le père présumé a un intérêt à être protégé contre des allégations concernant des circonstances très anciennes. D'autres intérêts peuvent être en jeu tels que la sécurité juridique ou les intérêts de tiers comme les membres de la famille du père présumé¹¹⁵.

L'introduction d'un délai pour introduire des procédures en matière de paternité peut se justifier par le souci d'assurer la sécurité juridique et les relations familiales. Par conséquent, l'existence d'un délai n'est pas en tant que tel incompatible. La Cour doit, par contre, vérifier si la nature de la prescription en question et/ou la manière dont elle est appliquée sont compatibles avec la Convention¹¹⁶.

À cet égard, la Cour prend en compte un certain nombre d'éléments lorsqu'elle réalise la mise en balance des intérêts en matière de prescription pour l'introduction de procédures en matière de paternité, comme le moment spécifique où le requérant est devenu conscient de la réalité biologique. La Cour examine par conséquent si les éléments qui fondent une action en paternité étaient remplis avant ou après l'expiration du délai de prescription. De plus, la Cour examine s'il existe un recours alternatif dans l'hypothèse où les actions sont prescrites. Cela peut comprendre par exemple la possibilité d'un recours interne effectif pour obtenir une extension de la prescription ou des exceptions à l'application de la prescription à des situations dans lesquelles une personne a eu connaissance de la réalité biologique après l'expiration de la prescription. Le critère contre lequel

¹¹³ Cour eur. D.H., décision du 17 octobre 2017, n° 54056/15, *Tadeusz Kordek c. Pologne*, § 28. Dans l'affaire *R.L et autres c. Danemark* (n° 52629/11), les requérants n'ont pas été empêchés d'introduire une demande de réouverture de la procédure pour une question de délai. Leur requête a été rejetée car la juridiction interne a procédé à une évaluation concrète qui l'a conduite à considérer que les conditions requises pour la réouverture des procédures en contestation de paternité n'étaient pas remplies.

¹¹⁴ Cour eur. D.H., arrêt du 3 octobre 2017, n° 72105/14 et 20415/15, *Silva et Mondim Correia c. Portugal*, § 51.

¹¹⁵ *Ibid.*, § 53.

¹¹⁶ *Ibid.*, § 57.

ces éléments sont mesurés est de savoir si une présomption légale a prévalu sur la réalité biologique et sociale et, dans l'affirmative, si, dans les circonstances du cas, c'est compatible avec l'obligation de garantir un respect effectif de la vie privée et familiale en tenant compte de la marge d'appréciation de l'État, des faits établis et des souhaits des personnes concernées¹¹⁷.

Dans le cas d'espèce, la Cour a considéré que l'impossibilité d'introduire une action en recherche de paternité était une ingérence dans le droit au respect de la vie privée et familiale¹¹⁸.

L. L'IDENTITÉ DES PERSONNES TRANSGENRES

L'identité sexuelle relève pleinement du droit au respect de la vie privée et cela vaut pour tous les individus¹¹⁹.

Les États membres ont l'obligation de reconnaître juridiquement la conversion sexuelle des personnes transsexuelles et leur marge d'appréciation ne peut porter que sur les conditions à remplir pour obtenir la reconnaissance juridique de leur nouvelle identité sexuelle et établir que leur conversion sexuelle a bien été opérée¹²⁰.

Dans le cas d'espèce qui lui était soumis, la Cour a considéré que conditionner la reconnaissance de l'identité sexuelle des personnes transgenres à la réalisation d'une opération ou d'un traitement stérilisant qu'elles ne souhaitaient pas subir, revient à conditionner le plein exercice de leur droit au respect de leur vie privée à la renonciation au plein exercice de leur droit au respect de leur intégrité physique que garantit non seulement cette disposition mais aussi l'article 3 de la Convention¹²¹. La Cour y a vu une rupture du juste équilibre que les États parties sont tenus de maintenir entre l'intérêt général et les intérêts des personnes concernées¹²².

Par ailleurs, la Cour a considéré que, même si un aspect important de l'identité des personnes transgenres était en cause, les États conservaient une large marge d'appréciation quant à la décision de poser comme condition un diagnostic préalable¹²³.

¹¹⁷ *Ibid.*, § 58.

¹¹⁸ *Ibid.*, § 59.

¹¹⁹ Cour eur. D.H., arrêt du 6 avril 2017, n^{os} 79885/12, 52471/13 et 52596/13, *A.P., Garçon et Nicot c. France*, §§ 92 et 95.

¹²⁰ *Ibid.*, § 97.

¹²¹ *Ibid.*, § 131.

¹²² *Ibid.*, § 132.

¹²³ *Ibid.*, § 140.

M. LA TRANSCRIPTION DES MARIAGES ENTRE PERSONNES
DE MÊME SEXE

En matière de mariages contractés à l'étranger par des personnes de même sexe, la Cour a énoncé qu'elle pouvait accepter dans le cas d'espèce que le refus de les enregistrer aurait été pris pour prévenir le désordre dans la mesure où le droit interne ne réglementait pas la situation des requérants¹²⁴. En l'absence de consensus au sein du Conseil de l'Europe, l'État doit se voir reconnaître une large marge d'appréciation à propos de la décision de reconnaître les mariages contractés à l'étranger¹²⁵. Ceci étant, dans la détermination de sa marge d'appréciation, la Cour doit aussi tenir compte du fait que l'affaire concerne des aspects importants de l'existence et de l'identité d'un individu¹²⁶.

En ce qui concerne les intérêts de l'État et de la société en général, la Cour peut accepter que l'Italie peut souhaiter empêcher ses ressortissants de recourir dans d'autres États à des institutions qui ne sont pas acceptées chez elle (comme les mariages entre personnes de même sexe) et qu'elle n'est pas obligée de reconnaître en vertu de la Convention. En effet, les affaires en cause sont la conséquence du choix du législateur italien de ne pas autoriser le mariage entre personnes de même sexe – choix qui n'est pas condamnable au regard de la Convention. Par conséquent, la Cour considère que l'État a un intérêt légitime à s'assurer que ces prérogatives législatives sont respectées et qu'en conséquence les choix pris par des gouvernements démocratiquement élus ne soient pas circonvenus¹²⁷. La Cour note que le refus de reconnaître ces mariages ne prive personne des droits antérieurement reconnus en Italie et que les mariés peuvent toujours bénéficier dans l'État dans lequel ils ont contracté mariage de tous les droits et obligations acquis en raison de ce mariage¹²⁸. Toutefois, la Cour note aussi que les décisions qui refusent la reconnaissance de leur mariage sous quelque forme que ce soit, laissent les requérants dans un vide juridique en ne prenant pas en considération la réalité sociale de la situation¹²⁹.

N. LA LIBERTÉ D'EXPRESSION, LA VIE PRIVÉE,
LA RÉPUTATION ET L'HONNEUR

1. *Les critères à prendre en considération lors de la mise en
balance des droits en présence*

Dans la droite ligne de sa jurisprudence antérieure, la Cour a rappelé un certain nombre de critères à prendre en considérant lors de la mise en balance des droits en présence : la contribution à un débat d'intérêt général, la notoriété de

¹²⁴ Cour eur. D.H., arrêt du 14 décembre 2017, n^{os} 26431/12, 26742/12, 44057/12 et 60088/12, *Orlandi et autres c. Italie*, § 200.

¹²⁵ *Ibid.*, §§ 204-205.

¹²⁶ *Ibid.*, § 206.

¹²⁷ *Ibid.*, § 207.

¹²⁸ *Ibid.*, § 208.

¹²⁹ *Ibid.*, § 209.

la personne visée, le sujet de la publication, le comportement antérieur de la personne concernée, le contenu, la forme et les répercussions de la publication¹³⁰, ainsi que, le cas échéant, les circonstances de l'espèce¹³¹, la manière dont l'information fut obtenue, sa véracité et la gravité de la sanction infligée¹³².

2. *La presse à sensation et la contribution à un débat d'intérêt général*

La Cour a répété que les publications ou émissions de télévision ayant pour seul objet de satisfaire la curiosité d'un certain public à l'égard de détails de la vie privée d'une personne, quelle que soit la notoriété de celle-ci, en s'immisçant dans son intimité, ne sauraient passer pour contribuer à un quelconque débat d'intérêt général pour la société. La Cour réaffirme à cet égard que l'intérêt général ne saurait être réduit aux attentes d'un public friand de détails quant à la vie privée d'autrui, ni au goût des lecteurs pour le sensationnel, voire pour le voyeurisme. Elle rappelle qu'une personne non publique dispose d'un droit plus large à préserver le secret de sa vie privée¹³³.

3. *La protection de la vie privée et les informations rendues publiques par la personne concernée*

Les informations portées à la connaissance du public par l'intéressé lui-même cessent d'être secrètes et deviennent librement disponibles, affaiblissant le degré de protection à laquelle ce dernier pouvait prétendre au titre de sa vie privée. Toutefois, toute tolérance réelle ou supposée d'un individu vis-à-vis de publications portant sur sa vie privée n'est pas de nature à le priver nécessairement de son droit à la protection de celle-ci¹³⁴.

Si la conduite de la personne avant la publication ou le fait que l'information ait déjà été publiée doit aussi être pris en compte, le simple fait d'avoir coopéré avec la presse à plusieurs reprises ne peut pas justifier que la personne soit privée de toute protection contre les publications¹³⁵.

¹³⁰ Cour eur. D.H., arrêt du 19 octobre 2017, n° 71233/13, *Fuschmann c. Allemagne*, § 50. La manière dont l'article est publié et la manière dont la personne concernée est représentée dans l'article doivent aussi être prises en considération. L'étendue de la diffusion de l'article est aussi un aspect important, à savoir : s'il s'agit d'un journal national ou local, s'il a une diffusion large ou limitée.

¹³¹ Cour eur. D.H., arrêt du 21 février 2017, n° 20996/10, *Rubio Dosamantes c. Espagne*, § 32; arrêt du 18 mai 2017, n° 25322/12, *Petrie c. Italie*, § 45; décision du 17 octobre 2017, n° 9483/15, *Sinem Hun c. Turquie*, § 21; arrêt du 21 novembre 2017, n° 63903/10, *Tarman c. Turquie*, § 38. Voy. aussi l'arrêt du 19 octobre 2017, n° 71233/13, *Fuschmann c. Allemagne*, §§ 34 et s.

¹³² Cour eur. D.H., arrêt du 16 mars 2017, n° 58493/13, *Olafsson c. Islande*, § 48.

¹³³ Cour eur. D.H., arrêt du 21 février 2017, n° 20996/10, *Rubio Dosamantes c. Espagne*, § 34.

¹³⁴ *Ibid.*, § 36.

¹³⁵ Cour eur. D.H., arrêt du 19 octobre 2017, n° 71233/13, *Fuschmann c. Allemagne*, § 48.

4. Une protection renforcée pour certains éléments de la vie privée

Certains événements de la vie privée et familiale font l'objet d'une protection particulièrement attentive au regard de l'article 8 et doivent conduire les journalistes à faire preuve de prudence et de précaution lors de leur traitement. Au demeurant, le fait de répandre de façon indiscriminée des rumeurs non vérifiées et de faire des commentaires, sans contrôle ni limite, sur n'importe quel sujet relatif à la vie privée d'autrui ne devrait pas être vu comme anodin¹³⁶.

5. Les obligations et responsabilités des médias

La requérante était l'éditeur d'un journal tenu pour civilement responsable pour la publication dans un journal. L'ingérence en cause doit dès lors être considérée dans le contexte de la fonction essentielle que les médias remplissent dans une société démocratique. Même si les médias ne doivent pas dépasser certaines limites, ils ont l'obligation de diffuser de manière consistante avec leurs obligations et responsabilités des informations et des idées sur toute matière d'intérêt public. Non seulement les médias ont la tâche de diffuser ces informations et idées, mais le public a également le droit de les recevoir. Les limites de la critique admissible sont plus étroites en ce qui concerne un citoyen privé qu'en ce qui concerne les politiciens des gouvernements¹³⁷.

En ce qui concerne la manière dont l'information a été obtenue et sa véracité, l'article 10 ne garantit pas une liberté d'expression sans restriction même lorsque la presse couvre des sujets d'intérêt public important. La liberté d'expression ne va pas sans obligations et responsabilités ce qui s'applique aussi aux médias même en ce qui concerne les sujets d'intérêt public important. La référence aux obligations et responsabilités signifie que pour être protégés par l'article 10 lorsqu'ils interviennent sur des sujets d'intérêt public, les journalistes doivent agir de bonne foi de manière à fournir des informations exactes et fiables conformément à l'éthique journalistique¹³⁸.

Toujours en ce qui concerne la manière dont l'information a été obtenue et sa véracité, le média a l'obligation de vérifier les affirmations de fait qui sont diffamatoires pour des personnes privées. Il doit considérer l'article dans son ensemble en portant une attention particulière aux mots utilisés dans les parties contentieuses des articles ainsi qu'au contexte dans lequel ils sont publiés, ainsi que la manière dont ils ont été préparés. La Cour contrôle si l'éditeur a agi de bonne foi et s'est assuré que les articles aient été écrits de manière conforme avec l'obligation journalistique de base de vérifier les faits. Cette obligation impose aux journalistes de se fonder sur une base factuelle suffisamment précise et fiable et qui

¹³⁶ Cour eur. D.H., arrêt du 21 février 2017, n° 20996/10, *Rubio Dosamantes c. Espagne*, § 41.

¹³⁷ Cour eur. D.H., arrêt du 25 avril 2017, n° 39748/05, *Ooo Izdatelskiy Tsentr Kvartirnyy Ryad c. Russie*, § 35.

¹³⁸ Cour eur. D.H., arrêt du 19 octobre 2017, n° 71233/13, *Fuschmann c. Allemagne*, § 42.

peut être considérée comme proportionnée à la nature et au degré des allégations, étant entendu qu'au plus l'allégation est sérieuse au plus la base factuelle doit être solide¹³⁹.

Les obligations et responsabilités qui incombent à la presse prennent d'autant plus de signification lorsqu'il est question de porter atteinte à la réputation d'un individu identifié et de porter atteinte aux droits d'autrui. Il faut donc des circonstances particulières pour que le média soit exempté de son obligation de vérifier les faits qui diffament des individus privés. Savoir si de telles circonstances existent dépend en particulier de la nature et du degré de diffamation et de la mesure dans laquelle le média peut raisonnablement considérer ses sources comme étant fiables au regard de ces allégations. Ceci doit être apprécié au vu de la situation telle que celle-ci se présente au journal au jour de la publication et ceci requiert la prise en compte d'autres éléments comme la fiabilité de la source, les investigations réalisées et la possibilité pour la personne diffamée de se défendre¹⁴⁰.

Lorsqu'elle contribue à un débat public sur des sujets d'intérêt légitime, la presse devrait normalement pouvoir se fier au contenu des documents officiels ou sur des informations fournies par un porte-parole du parquet sans avoir à accomplir de recherche complémentaire¹⁴¹.

L'article 10 protège non seulement le contenu des idées et informations émises mais également la forme sous laquelle elles sont diffusées. En conséquence, il n'appartient ni à la Cour ni aux juridictions nationales de substituer leur propre vue à celles de la presse sur les méthodes adoptées par les journalistes. La liberté journalistique couvre aussi le recours éventuel un certain degré d'exagération voire même de provocation¹⁴².

Une exigence faite aux journalistes de se distancier de manière systématique et formelle du contenu d'une citation qui est de nature à insulter ou provoquer d'autres personnes ou qui peut porter préjudice à leur réputation n'est pas compatible avec le rôle de la presse de fournir des informations sur des événements, opinions ou idées actuels. La sanction d'un journaliste pour avoir participé à la diffusion d'affirmations faites par une autre personne dans une interview pourrait sérieusement entraver la contribution de la presse au débat de sujets d'intérêt public et ne devrait pas être envisagée à moins qu'il n'y ait de raisons particulièrement fortes pour le faire¹⁴³.

¹³⁹ Cour eur. D.H., arrêt du 16 mars 2017, n° 58493/13, *Olafsson c. Islande*, § 53.

¹⁴⁰ Cour eur. D.H., arrêt du 19 octobre 2017, n° 71233/13, *Fuschmann c. Allemagne*, § 43.

¹⁴¹ *Ibid.*, § 44.

¹⁴² Cour eur. D.H., arrêt du 25 avril 2017, n° 39748/05, *Ooo Izdatelskiy Tsentri Kvartirnyy Ryad c. Russie*, § 36.

¹⁴³ Cour eur. D.H., arrêt du 16 mars 2017, n° 58493/13, *Olafsson c. Islande*, § 56.

6. La protection de la réputation et de l'honneur

Le droit à la protection de la réputation et de l'honneur est un droit protégé par l'article 8 – même si la personne fait l'objet de critiques dans le cadre d'un débat public. Pour que l'article 8 trouve à s'appliquer, l'atteinte à la réputation doit présenter un certain degré de gravité et être réalisée de manière à causer un préjudice à la jouissance personnelle du droit au respect de la vie privée¹⁴⁴.

Cette dernière exigence est importante puisque des millions d'utilisateurs d'Internet postent des commentaires en ligne tous les jours et beaucoup d'entre eux s'expriment de manière qui peut être vue comme étant offensive voire diffamatoire. Cependant, la majorité des commentaires sont plutôt triviaux et l'effet de leur publication est plutôt limité de sorte qu'ils ne causent pas de dommage significatif à la réputation d'autrui¹⁴⁵.

En ce qui concerne la question de savoir si l'atteinte à l'honneur personnel et à la réputation du requérant atteint le niveau requis de gravité pour que l'article 8 trouve à s'appliquer, la Cour a rappelé qu'en raison de la stigmatisation particulière attachée aux activités inspirées par le national-socialisme, toute allégation selon laquelle une personne aurait une relation ambiguë avec le national-socialisme représente un grief très sérieux¹⁴⁶.

Une personne ne peut invoquer l'article 8 pour se plaindre d'une atteinte à sa réputation qui résulterait de manière prévisible de ses propres actions telle qu'une infraction pénale¹⁴⁷.

7. La protection de la réputation et le contrôle de la balance des intérêts opérée par les juridictions nationales

Quand la Cour examine si l'ingérence dans la liberté d'expression est justifiée dans une société démocratique afin de protéger la réputation ou les droits d'autrui, elle peut devoir vérifier si les autorités nationales ont atteint un juste équilibre dans la protection de ces deux valeurs. Lorsque la mise en balance de ces deux droits a été réalisée par les autorités nationales conformément aux critères établis dans la jurisprudence de la Cour, il faut de sérieuses raisons pour que la Cour substitue son analyse à celles des juridictions nationales¹⁴⁸.

¹⁴⁴ Cour eur. D.H., arrêt du 16 mars 2017, n° 58493/13, *Olafsson c. Islande*, § 48; décision du 2 mai 2017, n° 55537/10, *Herbert Haupt c. Autriche*, § 28; arrêt du 18 mai 2017, n° 25322/12, *Petrie c. Italie*, § 39; arrêt du 20 juin 2017, n° 13812/09, *Bogomolova c. Russie*, § 51; décision du 19 septembre 2017, n° 3877/15, *Payam Tamiz c. Royaume-Uni*, § 77; décision du 17 octobre 2017, n° 9483/15, *Sinem Hun c. Turquie*, § 16; arrêt du 19 octobre 2017, n° 71233/13, *Fuschmann c. Allemagne*, § 30; arrêt du 7 novembre 2017, n° 24703/15, *Egill Einarsson c. Islande*, §§ 33-34; arrêt du 21 novembre 2017, n° 63903/10, *Tarman c. Turquie*, § 37.

¹⁴⁵ Cour eur. D.H., décision du 19 septembre 2017, n° 3877/15, *Payam Tamiz c. Royaume-Uni*, § 80.

¹⁴⁶ Cour eur. D.H., décision du 2 mai 2017, n° 55537/10, *Herbert Haupt c. Autriche*, § 28.

¹⁴⁷ Cour eur. D.H., décision du 4 avril 2017, n° 19557/05, *Hristo Nedkov Stoyanov c. Bulgarie*, § 43.

¹⁴⁸ Cour eur. D.H., arrêt du 25 avril 2017, n° 39748/05, *Ooo Izdatelskiy Tsentr Kvartirnyy Ryad c. Russie*, § 40; arrêt du 19 octobre 2017, n° 71233/13, *Fuschmann c. Allemagne*, § 31. Voy. la manière d'évaluer la marge d'appréciation dans la décision du 19 septembre 2017, n° 3877/15, *Payam Tamiz c. Royaume-Uni*, § 90.

Si cette mise en balance s'est faite dans le respect des critères établis dans la jurisprudence de la Cour, celle-ci doit essentiellement prêter attention à la motivation retenue par le juge national¹⁴⁹. Cette mise en balance n'est pas adéquate lorsque les juridictions nationales se sont contentées de vérifier la conformité du contenu des articles litigieux aux apparences et n'ont pas mis en balance de façon adéquate le droit de la requérante au respect de la vie privée et la liberté de la presse, conformément aux critères pertinents. Ainsi, dans le cas d'espèce, les décisions des juridictions nationales n'apportaient pas de réponse satisfaisante à la question de savoir si la liberté de la presse pouvait justifier l'atteinte portée au droit de la requérante à la protection de la réputation en raison de la forme et du contenu des articles litigieux en ce qu'ils révélaient l'identité et la photo de l'intéressée en la présentant comme une terroriste dangereuse, alors qu'elle n'était soupçonnée que de menaces et de chantages selon le dossier de l'enquête pénale menée par les autorités judiciaires¹⁵⁰.

8. La protection de la réputation des personnes publiques

La presse ne doit pas dépasser certaines limites notamment en ce qui concerne la réputation des droits d'autrui. Toutefois, les limites de la critique admissible sont plus larges en ce qui concerne un politicien qu'en ce qui concerne un individu privé. Contrairement à ce dernier, le premier s'expose inévitablement et consciemment à un contrôle plus étroit de chacun de ses faits et gestes tant par les journalistes que par le public en général. Il doit, en conséquence, montrer un plus grand degré de tolérance¹⁵¹.

De même, les personnes qui occupent des fonctions publiques doivent accepter le fait qu'elles seront soumises à un contrôle et à des critiques publiques notamment à travers les médias sur la manière dont ils ont exercé ou la manière dont ils exercent leurs fonctions dans la mesure de ce qui est nécessaire pour garantir la transparence et un exercice responsable de leurs fonctions. Les limites de la critique admissible sont plus larges en ce qui concerne un membre du gouvernement dans l'exercice de ses fonctions qu'en ce qui concerne un citoyen privé. La bonne gouvernance dans le secteur domanial et la prévention de la corruption sont des questions d'intérêt public¹⁵².

Même si le requérant n'était pas connu du grand public, son activité syndicale faisait de lui un personnage connu dans son secteur professionnel. Le fait qu'il avait été invité à intervenir devant la commission de l'emploi et des affaires sociales du Parlement européen atteste de sa notoriété. De plus, en intervenant ainsi au sein d'un débat d'intérêt public dans un cadre institutionnel interna-

¹⁴⁹ Cour eur. D.H., arrêt du 21 novembre 2017, n° 63903/10, *Tarman c. Turquie*, § 40.

¹⁵⁰ *Ibid.*, §§ 42-43.

¹⁵¹ Cour eur. D.H., décision du 2 mai 2017, n° 55537/10, *Herbert Haupt c. Autriche*, § 28; arrêt du 19 octobre 2017, n° 71233/13, *Fuschmann c. Allemagne*, § 40.

¹⁵² Cour eur. D.H., arrêt du 25 avril 2017, n° 39748/05, *Ooo Izdatelskiy Tsentri Kvartirny Ryad c. Russie*, § 38.

tional, le requérant s'était volontairement exposé à la critique et il devait, en conséquence, se montrer plus tolérant à l'égard de celle-ci¹⁵³.

En se présentant à des élections générales, une personne doit être considérée comme ayant inévitablement et consciemment entré le domaine public et s'exposer ainsi à un contrôle plus minutieux de ses actions. Les limites de la critique admissible doivent en conséquence être plus larges que dans le cas d'un individu privé¹⁵⁴.

9. La distinction entre les affirmations de fait et les jugements de valeur

Afin d'évaluer la justification d'une déclaration contestée, une distinction doit être opérée entre les affirmations de fait et les jugements de valeur. Si l'existence d'un fait peut être démontrée, par contre, la véracité d'un jugement de valeur n'est pas susceptible de preuve. L'exigence de prouver la véracité d'un jugement de valeur est impossible et viole la liberté d'expression en tant que telle. Classifier une déclaration comme un fait ou un jugement de valeur relève en premier lieu de la marge d'appréciation des autorités nationales et, en particulier, des juridictions nationales. Toutefois, même lorsqu'une déclaration constitue un jugement de valeur, il doit exister une base factuelle suffisante pour la fonder, à défaut de quoi elle sera excessive¹⁵⁵.

Même si la distinction entre déclaration de fait et jugement de valeur relève en premier de la marge d'appréciation des autorités nationales et, en particulier, des juridictions judiciaires, la Cour peut néanmoins considérer nécessaire qu'elle réalise elle-même sa propre appréciation des déclarations contestées¹⁵⁶ et vérifier si l'analyse de la juridiction nationale est bien dans les limites de la marge d'appréciation qui doit lui être reconnue dans la classification des déclarations¹⁵⁷.

Dans le cas d'espèce dont elle était saisie, le requérant était concerné par une déclaration libellée comme suit : « Fuck you rapist bastard ». En premier, la Cour a noté que le terme *violeur* était un terme objectif et factuel. Il se réfère directement à la personne qui a commis un acte de viol et qui est constitutif d'un crime au regard du code pénal islandais. La véracité d'une telle allégation de viol peut dès lors être prouvée. Il s'ensuit que *prima facie*, la déclaration « Fuck you rapist bastard » comprenait une déclaration de fait dès lors qu'elle attribuait le statut de violeur à la personne concernée par cette déclaration. Bien que la Cour n'ait pas exclu la possibilité qu'une déclaration factuelle objective comme celle en cause puisse contextuellement être classifiée comme représentant un jugement de valeur, les

¹⁵³ Cour eur. D.H., arrêt du 18 mai 2017, n° 25322/12, *Petrie c. Italie*, § 51.

¹⁵⁴ Cour eur. D.H., arrêt du 16 mars 2017, n° 58493/13, *Olafsson c. Islande*, § 51.

¹⁵⁵ Cour eur. D.H., arrêt du 25 avril 2017, n° 39748/05, *Ooo Izdatelskiy Tsentr Kvartirnyy Ryad c. Russie*, § 42 ; décision du 2 mai 2017, n° 55537/10, *Herbert Haupt c. Autriche*, § 28.

¹⁵⁶ Voy. : Cour eur. D.H., arrêt du 7 novembre 2017, n° 24703/15, *Egill Einarsson c. Islande*, §§ 48 et s.

¹⁵⁷ Voy. : *Ibid.*, § 49.

éléments contextuels justifiant une telle conclusion doivent être convaincants au regard de la nature objective et factuelle du terme *violeur* pris séparément¹⁵⁸. À cet égard, la Cour a considéré primordial que lorsque la juridiction nationale a décrit le contexte de la déclaration en question, elle se soit référée en premier à la participation du requérant dans un débat impitoyable qu'il avait lui-même initié. Toutefois, si la Cour n'a pas remis en question la constatation de la juridiction nationale selon laquelle la déclaration participait à un débat public impitoyable initié par le comportement du requérant et sa personnalité publique, elle a quand même souligné le fait que le contexte factuel dans lequel la déclaration a été faite et l'allégation selon laquelle le requérant était un violeur, était constitué par les procédures criminelles dans lesquelles le requérant était accusé de ce même crime et auxquelles la déclaration faisait référence, procédures qui ont été abandonnées par le procureur pour manque de preuves¹⁵⁹.

Au vu de ces éléments et, en particulier, de la nature objective et factuelle du terme *violeur* pris séparément, la Cour a considéré que l'appréciation contextuelle faite par la juridiction nationale ne s'appuyait pas sur des éléments pertinents et suffisants pour justifier sa conclusion selon laquelle la déclaration constituait un jugement de valeur.

Cependant, même à considérer que la déclaration était constitutive d'un jugement de valeur, la Cour a rappelé que, sous sa jurisprudence bien établie, même lorsqu'une déclaration constituait un jugement de valeur, il devait exister une base factuelle suffisante pour la supporter, à défaut de quoi elle serait excessive. Au vu de l'abandon des poursuites criminelles contre le requérant juste avant la publication de l'interview du requérant dans le journal, la juridiction nationale a donc échoué à expliquer de manière suffisante la base factuelle qui aurait permis de justifier l'appréciation selon laquelle le recours au terme *violeur* était constitutive d'un jugement de valeur¹⁶⁰.

En résumé, l'article 8 doit être interprété en ce sens que les personnes, même des personnes publiques contestées, qui ont initié un débat houleux en raison de leur comportement et de leurs commentaires publics, n'ont pas à tolérer d'être publiquement accusées d'actes criminels violents sans que ces affirmations ne soient supportées par des faits¹⁶¹.

10. La satire

La satire est une forme d'expression artistique et de commentaire social et, en raison de ses caractéristiques intrinsèques d'exagération et de distorsion de la réalité, est généralement destinée à provoquer et à agiter. Toute ingérence dans

¹⁵⁸ *Ibid.*, § 50.

¹⁵⁹ *Ibid.*, § 51.

¹⁶⁰ *Ibid.*, § 52.

¹⁶¹ *Ibid.*, §§ 48 et s.

le droit d'un artiste ou d'un commentateur social à s'exprimer doit être examinée avec un soin particulier même si le recours à cette forme d'expression n'écartera pas toute possibilité de restriction sous l'article 10, § 2, de la Convention¹⁶².

11. *Le contrôle en cas de sanctions*

Un contrôle très minutieux s'impose lorsque des mesures ou des pénalités sont capables de décourager la participation de la presse à des débats qui concernent des sujets d'intérêt public légitime. De plus, il faut des raisons particulièrement importantes pour toute mesure qui limite l'accès à l'information que le public a le droit de recevoir¹⁶³.

L'octroi de dommages-intérêts contre un éditeur représente une restriction à l'exercice du droit à la liberté d'expression¹⁶⁴.

Afin de savoir si l'ingérence peut être considérée comme nécessaire dans une société démocratique, la Cour vérifie l'adéquation et l'efficacité des protections contre les indemnités disproportionnées. En même temps, la Cour tient compte de la marge d'appréciation des juridictions nationales dans la mise en balance des intérêts et qui va de pair avec un contrôle européen. Dans l'exercice de sa fonction de contrôle, la tâche de la Cour n'est pas de prendre la place des juridictions nationales bien de contrôler si au regard de l'affaire considérée dans son ensemble les décisions prises dans le cadre de leur pouvoir d'appréciation sont compatibles avec les dispositions de la Convention en cause et si les raisons données pour les justifier sont pertinentes et suffisantes. Quand la mise en balance a été réalisée par les autorités nationales conformément aux critères établis par la jurisprudence de la Cour, il faut des raisons sérieuses pour que celle-ci substitue son point de vue à celui des juridictions nationales¹⁶⁵.

Il n'est pas nécessaire de se demander si les dommages-intérêts ont eu dans les faits un effet inhibiteur sur la presse. En règle, un montant d'indemnisation important et imprévisible est considéré comme pouvant avoir un tel effet et requiert dès lors un contrôle des plus stricts¹⁶⁶.

Dans l'espèce dont elle était saisie, la Cour a relevé que la première protection contre les indemnités disproportionnées prenait la forme des conseils donnés au jury sur la manière d'évaluer l'indemnisation à octroyer¹⁶⁷ et la seconde dans la possibilité d'interjeter appel¹⁶⁸.

¹⁶² Cour eur. D.H., décision du 2 mai 2017, n° 55537/10, *Herbert Haupt c. Autriche*, § 28.

¹⁶³ *Ibid.*, § 28.

¹⁶⁴ Cour eur. D.H., arrêt du 15 juin 2017, n° 28199/15, *Independent Newspapers (Ireland) Limited c. Irlande*, § 79.

¹⁶⁵ *Ibid.*, § 82.

¹⁶⁶ *Ibid.*, § 85.

¹⁶⁷ *Ibid.*, § 86.

¹⁶⁸ *Ibid.*, § 93.

12. *Le droit à la protection de son image*

En ce qui concerne les photographies, la Cour a déjà jugé que l'image d'une personne constituait un des principaux attributs de sa personnalité en ce que l'image révèle des caractéristiques uniques de la personne qui la distingue des autres. Le droit à la protection de l'image est donc un des éléments essentiels du développement personnel et il présuppose le droit de contrôler l'usage de cette image, en ce compris le droit de refuser sa publication¹⁶⁹.

13. *Le rôle des ONG comme « chien de garde social »*

Lorsqu'une ONG appelle l'attention de l'opinion sur des sujets d'intérêt public, elle exerce un rôle de chien de garde public semblable par son importance à celui de la presse et elle peut donc être qualifiée de « chien de garde » social, fonction qui justifie qu'elle bénéficie d'une protection similaire à celle accordée à la presse. La Cour a déjà reconnu l'apport important de la société civile au débat sur les affaires publiques¹⁷⁰.

À l'instar de la presse, une ONG jouant un rôle de chien de garde public aura probablement davantage d'impact lorsqu'elle signalera des irrégularités commises par des agents publics et elle disposera souvent de plus de moyens pour vérifier et corroborer la véracité des critiques ainsi alléguées qu'un particulier rapportant le fruit de ses observations personnelles. Elle doit aussi agir de bonne foi de manière à fournir des informations exactes et dignes de crédit dans le respect de la déontologie journalistique afin de pouvoir bénéficier de la protection de l'article 10¹⁷¹.

Dans la mise en balance des intérêts concurrents, la Cour estime approprié de tenir aussi compte des critères qui s'appliquent généralement à la diffusion de déclarations diffamatoires par les médias dans l'exercice de leur fonction de chien de garde public, à savoir le degré de notoriété de la personne concernée, l'objet du reportage, le contenu, la forme et les répercussions de la publication ainsi que le mode d'obtention des informations et leur véracité, et la gravité de la sanction imposée¹⁷².

14. *L'importance des archives en ligne*

La Cour a souligné la contribution importante des archives sur l'Internet pour préserver les informations et les rendre accessibles. De telles archives représentent une source importante pour l'éducation et la recherche historique, en particulier quand elles sont facilement accessibles au public – d'autant qu'elles sont géné-

¹⁶⁹ Cour eur. D.H., arrêt du 20 juin 2017, n° 13812/09, *Bogomolova c. Russie*, § 52.

¹⁷⁰ Cour eur. D.H. (GC), arrêt du 27 juin 2017, n° 17224/11, *Medzlis Islamske Zajednice Brcko et autres c. Bosnie Herzégovine*, § 86.

¹⁷¹ *Ibid.*, § 87.

¹⁷² *Ibid.*, § 88 (voy. les opinions dissidentes).

ralement gratuites¹⁷³. Mais, en même temps, le risque de causer un dommage à l'exercice et à la jouissance des droits et libertés (en particulier, le droit au respect de la vie privée), est certainement plus élevé que celui posé par la presse¹⁷⁴.

15. *La non-responsabilité des fournisseurs de services de la société de l'information*

Il est communément admis que les fournisseurs de services Internet ne devraient pas être tenus responsables du contenu qui émane de tiers, à moins que ces fournisseurs aient manqué à leur obligation d'agir de manière diligente en enlevant ou en désactivant l'accès à des contenus une fois qu'ils sont conscients de leur caractère illégal¹⁷⁵. La Cour a rappelé que l'arrêt rendu dans l'affaire *Delfi* ne concernait pas l'hypothèse dans laquelle le fournisseur de la plate-forme ne fournissait aucun contenu¹⁷⁶.

O. LA PROTECTION DES COMMUNICATIONS TÉLÉPHONIQUES EN PRISON

L'article 8 ne garantit pas aux prisonniers le droit à des appels téléphoniques en tant que tel notamment s'il existe d'autres possibilités appropriées pour une correspondance écrite. S'il existe des équipements téléphoniques disponibles, ils peuvent faire l'objet de restrictions conformément aux contraintes ordinaires et raisonnables liées à l'emprisonnement¹⁷⁷. Ceci étant, toute restriction est une ingérence dans les droits du détenu sous l'article 8 et doit, en conséquence, être justifiée¹⁷⁸.

II. La protection des données dans la jurisprudence du Tribunal et de la Cour de justice de l'Union européenne

A. LE CHAMP D'APPLICATION MATÉRIEL DE LA DIRECTIVE 95/46/CE

Dans un arrêt du 27 septembre 2017, la C.J.U.E. a abordé la question du champ d'application matériel de la directive et, plus particulièrement, de l'exception visée à son article 3.2 qui exclut l'application de la directive pour les traitements « ayant pour objet la sécurité publique, la défense, la sûreté de l'État (y compris le bien-être économique de l'État lorsque ces traitements) »¹⁷⁹. Elle a ainsi eu l'occasion de

¹⁷³ Cour eur. D.H., arrêt du 19 octobre 2017, n° 71233/13, *Fuschmann c. Allemagne*, § 39.

¹⁷⁴ Cour eur. D.H., arrêt du 7 novembre 2017, n° 24703/15, *Egill Einarsson c. Islande*, § 46.

¹⁷⁵ Cour eur. D.H., décision du 19 septembre 2017, n° 3877/15, *Payam Tamiz c. Royaume-Uni*, § 84.

¹⁷⁶ *Ibid.*, § 85.

¹⁷⁷ Cour eur. D.H., arrêt du 19 octobre 2017, n° 67482/14, *Lebois c. Bulgarie*, § 61.

¹⁷⁸ *Ibid.*, § 62.

¹⁷⁹ Article 3.2 de la directive 95/46.

rappeler sa jurisprudence antérieure qui précise que « en tant qu'elle rend inapplicable le régime de protection des données à caractère personnel prévu par la directive 95/46 et s'écarte ainsi de l'objectif sous-jacent à celle-ci, consistant à assurer la protection des libertés et des droits fondamentaux des personnes physiques à l'égard du traitement des données à caractère personnel, l'exception prévue à l'article 3, paragraphe 2, premier tiret, de cette directive doit faire l'objet d'une interprétation stricte »¹⁸⁰.

Après ce rappel, elle a précisé que « sous réserve des vérifications à effectuer à cet égard par la juridiction de renvoi, il n'apparaît cependant pas que le traitement [des données collectées et utilisées aux fins de la perception de l'impôt et de la lutte contre la fraude fiscale] a pour objet la sécurité publique, la défense ou la sûreté de l'État »¹⁸¹.

B. LA NOTION DE DONNÉE À CARACTÈRE PERSONNEL

Dans un arrêt du 20 décembre 2017, la Cour a eu l'occasion d'analyser la notion de donnée à caractère personnel dans le cadre d'une demande de consultation de son examen professionnel par un candidat¹⁸² après, entre autres, que le Commissaire à la protection des données irlandais ait considéré que les informations figurant dans une copie corrigée d'examen ne constituaient pas des données à caractère personnel.

La Cour rappelle que « pour qu'une donnée puisse être qualifiée de "donnée à caractère personnel", au sens de l'article 2, sous a), de la directive 95/46, il n'est pas requis que toutes les informations permettant d'identifier la personne concernée se trouvent entre les mains d'une seule personne (arrêt du 19 octobre 2016, *Breyer*, C-582/14, EU:C:2016:779, point 43). Il est par ailleurs constant que, dans l'hypothèse où l'examineur ne connaît pas l'identité du candidat lors de la notation des réponses fournies par celui-ci dans le cadre d'un examen, l'entité organisant l'examen, en l'occurrence l'ordre des experts-comptables, dispose, en revanche, des informations nécessaires lui permettant d'identifier sans difficultés ou doutes ce candidat à partir de son numéro d'identification, apposé sur la copie d'examen ou le feuillet de couverture de cette copie, et ainsi de lui attribuer ses réponses »¹⁸³.

Elle poursuit en rappelant que « le champ d'application de la directive 95/46 est très large et les données à caractère personnel visées par celle-ci sont variées (arrêt du 7 mai 2009, *Rijkeboer*, C-553/07, EU:C:2009:293, point 59 et jurisprudence citée) »¹⁸⁴ et que l'utilisation du vocable de « toute information » pour

¹⁸⁰ C.J.U.E., 27 septembre 2017, *Peter Puškár c. Finančné riaditeľstvo Slovenskej republiky, Kriminálny úrad finančnej správy*, C-73/16, § 38.

¹⁸¹ *Ibidem*, § 39.

¹⁸² C.J.U.E., 20 décembre 2017, *Peter Nowak c. Data Protection Commissioner*, C-434/16.

¹⁸³ *Ibidem*, § 31.

¹⁸⁴ *Ibidem*, § 33.

définir une donnée à caractère personnel montre la volonté du législateur européen de donner un sens large à cette notion ; notion qui « n'est pas restreinte aux informations sensibles ou d'ordre privé, mais englobe potentiellement toute sorte d'informations, tant objectives que subjectives sous forme d'avis ou d'appréciations, à condition que celles-ci "concernent" la personne en cause »¹⁸⁵.

Au terme de ces rappels, la Cour considère que « les réponses écrites fournies par un candidat à un examen professionnel constituant de telles informations liées à sa personne »¹⁸⁶ dès lors que

■ « le contenu de ces réponses reflète le niveau de connaissance et de compétence du candidat dans un domaine donné ainsi que, le cas échéant, ses processus de réflexion, son jugement et son esprit critique. En cas d'examen rédigé à la main, les réponses contiennent, en outre, des informations calligraphiques.

Ensuite, la collecte desdites réponses a pour finalité d'évaluer les capacités professionnelles du candidat et son aptitude à exercer le métier en cause.

Enfin, l'utilisation de ces informations, qui se traduit, notamment, par le succès ou l'échec du candidat à l'examen concerné, est susceptible d'avoir un effet sur les droits et intérêts de celui-ci, en ce qu'elle peut déterminer ou influencer, par exemple, ses chances d'accéder à la profession ou à l'emploi souhaités »¹⁸⁷. ■

Par ailleurs, il en va de même pour les annotations de l'examineur dès lors qu'elles constituent des informations concernant le candidat¹⁸⁸.

C. LA NOTION DE RESPONSABLE DE TRAITEMENT

Les conclusions de l'avocat général Yves Bot dans une affaire *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein contre Wirtschaftsakademie Schleswig-Holstein GmbH* sont intéressantes car elles s'attachent à définir la notion de responsable du traitement et celle de responsabilité conjointe au sens de la directive 95/46¹⁸⁹.

Il s'agit d'une cause opposant une société spécialisée dans le domaine de l'éducation, la *Wirtschaftsakademie*, à l'autorité régionale de protection des données de Schleswig-Holstein qui l'avait enjoint de désactiver une « fan page » hébergée sur le site de Facebook Ireland. En effet, la *Wirtschaftsakademie* exploitait une fan page lui permettant d'établir des statistiques d'audience grâce à l'outil « Facebook Insights » pour ensuite diffuser de la publicité ciblée.

¹⁸⁵ *Ibidem*, § 34.

¹⁸⁶ *Ibidem*, § 36.

¹⁸⁷ *Ibidem*, §§ 37-39.

¹⁸⁸ *Ibidem*, § 42.

¹⁸⁹ La C.J.U.E. a rendu son arrêt le 5 juin 2018 qui est conforme aux conclusions de l'avocat général (C.J.U.E. (GC), C-210/16, <http://curia.europa.eu>).

Ainsi que l'explique l'avocat général¹⁹⁰ :

■ « 17. Les administrateurs de pages fan peuvent obtenir des statistiques d'audience à l'aide de l'outil "Facebook Insights" mis gratuitement à leur disposition par Facebook dans le cadre des conditions d'utilisation non modifiables. Ces statistiques sont élaborées par Facebook et personnalisées par l'administrateur d'une page fan à l'aide de différents critères qu'il peut sélectionner, tels que l'âge ou le sexe. Lesdites statistiques fournissent ainsi des informations anonymes sur les caractéristiques et les habitudes des personnes ayant consulté les pages fan, permettant aux administrateurs de ces pages de mieux cibler leur communication.

18. Afin d'établir de telles statistiques d'audience, au moins un cookie comportant un numéro ID unique, qui est actif pendant deux ans, est sauvegardé par Facebook sur le disque dur de la personne ayant consulté la page fan. Le numéro ID, qui peut être mis en relation avec les données de connexion des utilisateurs enregistrés sur Facebook, est collecté et traité au moment de l'ouverture des pages Facebook ».

La cause a été introduite par l'autorité régionale de protection des données de Schleswig-Holstein suite à une décision du tribunal administratif puis par le tribunal administratif supérieur allemand invalidant une injonction qu'elle avait adressée à la *Wirtschaftsakademie*, au motif que cette dernière ne pouvait pas être considérée comme organisme responsable au sens de de l'article 3, paragraphe 7, du BDSG¹⁹¹. La Cour administrative fédérale n'a pas fait droit au recours introduit par l'autorité régionale de protection des données de Schleswig-Holstein en considérant que la « *Wirtschaftsakademie* ne répondrait pas à [la définition de responsable de traitement énoncée à l'article 2, d, de la directive 95/46] dans la mesure où elle n'a aucune influence en droit ou en fait sur les modalités du traitement des données à caractère personnel qui est effectué par l'intervenante au principal sous sa propre responsabilité et en toute indépendance. À cet égard, serait insuffisante la circonstance que la *Wirtschaftsakademie* peut objectivement tirer profit de la fonction "Facebook Insights" exploitée par l'intervenante au principal au motif que des données rendues anonymes lui sont transmises en vue de l'utilisation de sa page fan »¹⁹².

Il est intéressant de lire la description de l'utilisation de l'outil « Facebook Insights » donnée par l'avocat général¹⁹³ :

■ « Bien que les finalités et les modalités de l'outil "Facebook Insights" en tant que tel soient définies de façon générale par Facebook Inc. conjointement avec

¹⁹⁰ C.J.U.E., 14 avril 2016, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein c. Wirtschaftsakademie Schleswig-Holstein GmbH*, aff. C-210/16, conclusions de l'avocat général Yves Bot (24 octobre 2017), §§ 17-18.

¹⁹¹ « On entend par organisme responsable toute personne ou tout organisme qui collecte, traite ou utilise des données à caractère personnel pour son compte ou par l'intermédiaire d'autrui en sous-traitance ».

¹⁹² *Ibidem*, § 28.

¹⁹³ *Ibidem*, § 57.

Facebook Ireland, l'administrateur d'une page fan a la possibilité d'influer sur la mise en œuvre concrète de cet outil en définissant les critères à partir desquels les statistiques d'audience sont établies. Lorsque Facebook invite l'administrateur d'une page fan à créer ou à modifier l'audience de sa page, il lui indique qu'il fera de son mieux pour montrer cette page aux personnes qui comptent le plus pour lui. L'administrateur d'une page fan peut, à l'aide de filtres, définir une audience personnalisée, ce qui lui permet non seulement d'affiner le groupe de personnes à destination duquel des informations relatives à son offre commerciale seront diffusées, mais surtout de désigner les catégories de personnes qui vont faire l'objet d'une collecte de leurs données à caractère personnel par Facebook. Ainsi, en déterminant l'audience qu'il souhaite toucher, l'administrateur d'une page fan identifie par la même occasion quel public cible est susceptible de faire l'objet d'une collecte puis d'une exploitation de ses données à caractère personnel par Facebook. En plus d'être l'élément déclencheur d'un traitement de telles données lorsqu'il crée une page fan, l'administrateur de cette page joue dès lors un rôle prépondérant dans la mise en œuvre de ce traitement par Facebook. Il prend part, de la sorte, à la détermination des moyens et des finalités dudit traitement en exerçant sur celui-ci une influence de fait. ■

Au terme de ce raisonnement et de la considération que le réseau social hébergeant la page et l'administrateur de cette même page poursuivent des finalités étroitement liées, l'avocat général Bot considère que l'administrateur d'une « fan page » sur Facebook doit être considéré comme responsable de traitement conjoint avec Facebook, son rôle de responsable du traitement se limitant cependant à la phase de collecte des données relatives aux personnes qui consultent ladite page. En corollaire, il réaffirme le principe selon lequel le juge peut se départir de la qualification donnée par les parties.

En outre et cela est intéressant, il précise que¹⁹⁴:

« il n'est pas nécessaire que cette personne dispose d'un pouvoir de contrôle complet sur tous les aspects du traitement. Comme le gouvernement belge l'a indiqué à juste titre lors de l'audience, un tel contrôle existe de moins en moins en pratique. De plus en plus, les traitements ont une nature complexe, en ce sens qu'il s'agit de plusieurs traitements distincts impliquant plusieurs parties exerçant elles-mêmes différents degrés de contrôle. Par conséquent, l'interprétation privilégiant l'existence d'un pouvoir de contrôle complet sur tous les aspects du traitement est susceptible d'entraîner de sérieuses lacunes en matière de protection des données à caractère personnel ». ■

Il opte, par là-même, pour une interprétation large de la notion de responsable du traitement afin d'éviter les abus et éviter ainsi de voir un responsable du traitement faire appel à un tiers pour contourner ses responsabilités. Il précise cependant qu'« une responsabilité conjointe ne signifie pas une responsabilité sur un

¹⁹⁴ Ibidem, § 62.

pied d'égalité. Au contraire, les différents responsables du traitement peuvent être impliqués dans un traitement de données à caractère personnel à différents stades et à différents degrés»¹⁹⁵.

À noter que l'avocat général Bot étend son raisonnement aux exploitants de sites Internet qui utilisent le service « Facebook Insights » ou similaire pour obtenir des statistiques liées aux visiteurs de leur site en intégrant le bouton « j'aime ».

D. LA LÉGITIMATION/LICÉITÉ DES TRAITEMENTS DE DONNÉES

L'affaire *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde* (bureau d'examen des infractions administratives à la circulation du département de la police de maintien de l'ordre du département de la police nationale du district de Riga, Lettonie) contre *Rīgas pašvaldības SIA «Rīgas satiksme»* (société de trolleybus de la ville de Riga, Lettonie)¹⁹⁶ concerne une demande de données d'identification de l'auteur d'un accident par la seconde nommée à la première afin de pouvoir introduire une action civile en responsabilité suite à un accident de roulage au cours duquel un trolleybus avait été endommagé par l'ouverture d'une portière de taxi par le passager. La police de Riga refusait de communiquer l'identité complète ainsi que les déclarations contenues dans le dossier administratif ouvert à l'occasion de cet accident se contentant de ne communiquer que les nom et prénom du passager. Le Tribunal administratif saisi par la société de trolley a donné raison à cette dernière et a ordonné à la police de faire droit à la demande de communication des données.

La Cour de cassation saisie par la police nationale a demandé l'avis à l'autorité nationale de la protection des données lettone qui a considéré que « l'article 7, point 6, de la loi relative à la protection des données des personnes physiques ne peut pas servir de base juridique à la communication des données à caractère personnel dans le litige au principal, car le code letton des infractions administratives énumère les personnes auxquelles la police nationale peut communiquer les informations relatives à une affaire »¹⁹⁷.

Peu convaincue, la Cour de cassation lettone a posé une question préjudicielle à la Cour sur, entre autres, l'interprétation devant être donnée sur l'expression « il est nécessaire à la réalisation de l'intérêt légitime poursuivi [...] par le ou les tiers auxquels les données sont communiquées » visée à l'article 7, sous f), de la directive 95/46. Doit-elle être interprétée en ce sens que la police est tenue de communiquer à la société de trolleybus les données à caractère personnel deman-

¹⁹⁵ *Ibidem*, § 75.

¹⁹⁶ C.J.U.E., 4 mai 2017, *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde c. Rīgas pašvaldības SIA «Rīgas satiksme»*, C-13/16.

¹⁹⁷ *Ibidem*, p. 5, § 18.

dées et qui sont nécessaires à l'introduction d'une requête dans une procédure de droit civil?

La Cour a rappelé que «L'article 7, sous f), de la directive 95/46 prévoit trois conditions cumulatives pour qu'un traitement de données à caractère personnel soit licite, à savoir, premièrement, la poursuite d'un intérêt légitime par le responsable du traitement ou par le ou les tiers auxquels les données sont communiquées, (...)»¹⁹⁸.

Ramenant cette notion au cas d'espèce, il a considéré que¹⁹⁹:

■ «il ne fait aucun doute que l'intérêt d'un tiers à obtenir une information d'ordre personnel concernant une personne qui a porté atteinte à sa propriété afin de l'assigner en justice pour obtenir réparation constitue un intérêt légitime (voir, en ce sens, arrêt du 29 janvier 2008, *Promusicae*, C-275/06, EU:C:2008:54, point 53). Cette analyse est confortée par l'article 8, paragraphe 2, sous e), de la directive 95/46 qui prévoit que l'interdiction du traitement de certains types de données à caractère personnel, telles que celles qui révèlent l'origine raciale ou les convictions politiques, ne s'applique pas notamment lorsque le traitement est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice».

Elle a considéré que l'article 7, sous f), de la directive 95/46 «doit être interprété en ce sens qu'il n'impose pas l'obligation de communiquer des données à caractère personnel à un tiers afin de lui permettre d'introduire un recours en indemnisation devant une juridiction civile pour un dommage causé par la personne concernée par la protection de ces données. Toutefois, l'article 7, sous f), de cette directive ne s'oppose pas à une telle communication sur la base du droit national»²⁰⁰ comme le prétendait l'autorité lettone.

Dans la cause *Peter Puškár c. Finančné riaditeľstvo Slovenskej republiky, Kriminálny úrad finančnej správy*²⁰¹, la Cour a analysé la notion de «traitement nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, dont est investi le responsable du traitement» prévue à l'article 7, e, de la directive 95/46.

En l'espèce, la direction des finances et le bureau de lutte contre la criminalité financière avaient établi et utilisaient une liste de personnes considérées par la direction des finances comme des prête-noms; liste établie dans le cadre de la perception de l'impôt et dont la mise à jour était assurée par la direction des

¹⁹⁸ *Ibidem*, p. 5, § 28.

¹⁹⁹ *Ibidem*, p. 5, § 29.

²⁰⁰ *Ibidem*, p. 5, § 34.

²⁰¹ C.J.U.E., 27 septembre 2017, *Peter Puškár c. Finančné riaditeľstvo Slovenskej republiky, Kriminálny úrad finančnej správy*, C-73/16.

finances, les bureaux des impôts qui lui sont subordonnés ainsi que le bureau de lutte contre la criminalité financière²⁰².

La Cour a rappelé qu'il appartenait aux juridictions nationales de vérifier si le traitement opéré était nécessaire à l'exécution de missions d'intérêt public et donc « de veiller au respect du principe de proportionnalité »²⁰³ en précisant que « la protection du droit fondamental au respect de la vie privée au niveau de l'Union exige que les dérogations à la protection des données à caractère personnel et les limitations de celle-ci s'opèrent dans les limites du strict nécessaire (voir, en ce sens, arrêt du 21 décembre 2016, *Tele2 Sverige et Watson e.a.*, C-203/15 et C-698/15, EU:C:2016:970, point 96 ainsi que jurisprudence citée) »²⁰⁴. En d'autres termes, les juridictions nationales doivent « vérifier si l'établissement de la liste litigieuse et l'inscription sur celle-ci du nom des personnes concernées sont propres à réaliser les objectifs poursuivis par ceux-ci et s'il n'existe pas d'autres moyens moins contraignants afin d'atteindre ces objectifs »²⁰⁵. De plus, l'autorité se prévalant d'une telle base de légitimité/licéité doit avoir « été investie par la législation nationale de missions d'intérêt public au sens de cette disposition »²⁰⁶.

E. LA CONSERVATION DES DONNÉES

La Cour a eu l'occasion de se pencher sur la question de la conservation des données à caractère personnel sous une forme permettant l'identification des personnes concernées au sens de l'article 6, 1, e, de la directive 95/46.

Le litige était lié à une demande de radiation, d'anonymisation ou de blocage de donnée liant le demandeur à la faillite d'une société et contenue dans le registre des sociétés de la Chambre de commerce de Lecce (Italie). En effet, ces données avaient été utilisées par une société spécialisée dans la collecte et le traitement d'informations de marché et dans l'évaluation des risques (rating).

Si le Tribunal de Lecce avait fait droit à cette demande considérant que « les inscriptions qui lient le nom d'une personne physique à une phase critique de la vie de l'entreprise (comme la faillite) ne peuvent être pérennes, à défaut d'un intérêt général spécifique à leur conservation et divulgation »²⁰⁷, la Cour de cassation a, avant de se prononcer, posé deux questions préjudicielles à la C.J.U.E. dont une sur l'articulation entre le principe de conservation des données à caractère personnel sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées (l'article 6, 1, e, de la directive 95/46) et le

²⁰² *Ibidem*, § 2.

²⁰³ *Ibidem*, § 112.

²⁰⁴ *Ibidem*, § 112.

²⁰⁵ *Ibidem*, § 113.

²⁰⁶ *Ibidem*, § 117.

²⁰⁷ C.J.U.E., 9 mars 2017, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce c. Salvatore Manni*, C-398/15, point 27.

système de publicité mis en place avec le registre des sociétés, prévu par la directive 68/151 tendant à coordonner, pour les rendre équivalentes, les garanties qui sont exigées dans les États membres, des sociétés au sens de l'article 58 deuxième alinéa du traité, pour protéger les intérêts tant des associés que des tiers abrogé depuis 2009.

Après avoir rappelé qu'« ainsi qu'il résulte de son article 1^{er} et de son considérant 10, celle-ci vise à garantir un niveau élevé de protection des libertés et des droits fondamentaux des personnes physiques, notamment de leur vie privée, à l'égard du traitement des données à caractère personnel (voir arrêt du 13 mai 2014, *Google Spain et Google*, C-131/12, EU:C:2014:317, point 66 ainsi que jurisprudence citée) »²⁰⁸, le Cour a analysé l'économie de la directive 68/151 qui avait pour objectif de permettre de garantir la sécurité juridique entre les sociétés et les tiers; tiers qui doivent pouvoir « aisément prendre connaissance des données essentielles relatives à la constitution des sociétés commerciales et aux pouvoirs des personnes chargées de les représenter, ce qui nécessite que toutes les données pertinentes figurent de manière explicite dans le registre (voir, en ce sens, arrêt du 12 novembre 1974, *Haaga*, 32/74, EU:C:1974:116, point 6) »²⁰⁹. Elle a ensuite constaté que, même si la société n'existait plus suite à une faillite par exemple, des tiers pouvaient cependant encore avoir besoin d'informations la concernant pour établir des faits intervenus lors de son existence.

Elle conclut de cette analyse qu'il est donc difficile de fixer un délai de conservation des données à caractère personnel unique et qu'il appartient aux tribunaux nationaux de vérifier l'état de leur droit sur cette notion de conservation mais également et en corollaire sur le droit d'opposition qui serait formulée par une personne concernée sur base de l'article 14 de la directive 95/46. Cette vérification devra s'effectuer au « regard de l'ensemble des circonstances pertinentes et en tenant compte du délai écoulé depuis la dissolution de la société concernée, l'existence éventuelle de raisons prépondérantes et légitimes qui seraient, le cas échéant, de nature à justifier exceptionnellement de limiter l'accès des tiers aux données concernant [la personne concernée] dans le registre des sociétés »²¹⁰.

F. DROIT À UN RECOURS JURIDICTIONNEL

Dans l'affaire *Peter Puškár c. Finančné riaditeľstvo Slovenskej republiky, Kriminálny úrad finančnej správy*²¹¹, la Cour s'est également penché sur la question du droit à un recours juridictionnel. En effet, le droit slovaque imposait des recours administratifs préalables à un recours devant les juridictions judiciaires. En d'autres termes, un recours judiciaire n'était recevable qu'à la condition que les voies de

²⁰⁸ *Ibidem*, § 37.

²⁰⁹ *Ibidem*, § 50.

²¹⁰ *Ibidem*, § 63.

²¹¹ C.J.U.E., 27 septembre 2017, *Peter Puškár c. Finančné riaditeľstvo Slovenskej republiky, Kriminálny úrad finančnej správy*, C-73/16.

recours administratives aient été préalablement épuisées. La Cour a considéré que le droit slovaque imposait une étape supplémentaire pour l'accès au juge ce qui retardait l'accès à un recours juridictionnel en engendrant, de plus, des coûts complémentaires²¹². Cependant, cela est acceptable si « l'obligation d'épuiser les voies de recours administratives disponibles répond à un objectif d'intérêt général et si, dans l'affirmative, elle respecte le principe de proportionnalité au sens de l'article 52, paragraphe 1, de la Charte [des droits fondamentaux de l'Union européenne] »²¹³. En clair, « l'article 47 de la Charte des droits fondamentaux de l'Union européenne doit être interprété en ce sens qu'il ne s'oppose pas à une législation nationale qui subordonne l'exercice d'un recours juridictionnel par une personne affirmant qu'il a été porté atteinte à son droit à la protection des données à caractère personnel garanti par la directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, à l'épuisement préalable des voies de recours disponibles devant les autorités administratives nationales, à condition que les modalités concrètes d'exercice desdites voies de recours n'affectent pas de manière disproportionnée le droit à un recours effectif devant un tribunal visé à cette disposition »²¹⁴. Cela ne doit cependant pas entraîner « de retard substantiel pour l'introduction d'un recours juridictionnel, [doit] entraîner la suspension de la prescription des droits concernés et [ne doit pas occasionner] de frais excessifs »²¹⁵.

G. COMPÉTENCES DES AUTORITÉS DE CONTRÔLE

L'avocat général Bot a, dans ses conclusions présentées le 24 octobre 2017 dans l'affaire *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein contre Wirtschaftsakademie Schleswig-Holstein GmbH* déjà analysée ci-dessus, déduit de l'article 4, paragraphe 1, a, de la directive 95/46 que « la structure d'un groupe caractérisée par la présence d'établissements du responsable du traitement dans plusieurs États membres ne doit pas avoir pour effet de permettre à ce dernier de contourner le droit de l'État membre dans le ressort duquel chacun de ces établissements est établi »²¹⁶. Il considère par ailleurs que « l'interprétation favorable à l'application exclusive du droit de l'État membre dans lequel se situe le siège européen d'un groupe international ne peut plus, à [son] avis être défendue depuis l'arrêt du 28 juillet 2016, *Verein für Konsumenteninformation* [C-191/15, EU:C:2016:612] »²¹⁷. Il a ainsi rappelé que la règle du shopping consistant à choisir le pays dans lequel l'autorité de protection est la plus souple pour établir son siège européen ne peut être suivie. Il faudra voir ce qu'il en sera avec le nouveau règlement européen pour la protection des données (RGPD ou GDPR).

²¹² *Ibidem*, § 61.

²¹³ *Ibidem*, § 65.

²¹⁴ *Ibidem*, dispositif de l'arrêt.

²¹⁵ *Idem*.

²¹⁶ C.J.U.E., 14 avril 2016, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein c. Wirtschaftsakademie Schleswig-Holstein GmbH*, § 100.

²¹⁷ *Idem*.

Pour aboutir à cette conclusion, l'avocat général a procédé à une analyse de la situation de Facebook en Europe et s'est appuyé, entre autres, sur l'avis 8/2010 sur le droit applicable du 16 décembre 2010 du Groupe de travail de l'article 29. Il a donc rappelé que l'applicabilité de la loi nationale d'un État membre transposant la directive 95/46 suppose la réunion de deux conditions étant un « établissement » du responsable du traitement dans cet État membre et que le traitement ait lieu « dans le cadre des activités » de cet établissement²¹⁸.

Jean Herveg

Directeur de Recherche au Centre de Recherches Information, Droit et Société
Avocat au barreau de Bruxelles
Auteur de la partie consacrée à la Cour européenne des droits de l'homme

Jean-Marc Van Gyseghem

Directeur de Recherche au Centre de Recherches Information, Droit et Société
Avocat Barreau de Bruxelles
Auteur de la partie consacrée aux juridictions de l'Union européenne

²¹⁸ *Ibidem*, § 88.